Grado en Ingeniería Informática

Departamento de Informática

Especialidad: Sistemas de la Información

TRABAJO FIN DE GRADO

METODOLOGÍA PARA LA MEDICIÓN DE INDICADORES DE SEGURIDAD

Autor: Víctor García de León González

Tutor: Juan Miguel Gómez Berbís
Cotutor: José María Álvarez Rodríguez

Fecha: 07/07/2015

Agradecimientos

Con la entrega de este trabajo se cierra una etapa de mi vida y comienza otra nueva con muchas ganas e ilusión por mi parte. La etapa universitaria ha sido dura y en algunos momentos muy costosa, pero ha llegado el momento de la recompensa.

En primer lugar me gustaría agradecer a mi tutor Juan Miguel Gómez Berbís la posibilidad de haber realizado este trabajo y a mi cotutor, José María Álvarez Rodríguez, por la gran ayuda que me ha ofrecido.

A lo largo de la etapa universitaria he tenido el placer de conocer a muchos profesores que me han aportado grandes conocimientos que me serán muy útiles a lo largo de mi vida profesional. Afortunadamente he tenido la suerte de contar con unos grandes compañeros durante la carrera que me han ayudado siempre que lo he necesitado. Destacar a Roberto y Ana, con los que he compartido especialmente los dos últimos años de la carrera y hoy considero grandes amigos.

En el ámbito personal he de agradecer a mis padres, hermano y abuelo el apoyo que me han ofrecido durante este periodo. A mis padres por haberme ofrecido siempre la oportunidad de formarme en todo lo que he necesitado para convertirme en lo que soy hoy en día. Merece un agradecimiento especial mi madre, mi referente a seguir en la vida y cuyo apoyo y ayuda es indispensable en mi día a día. También me gustaría recordar a aquellos miembros de mi familia que hoy ya no están pero seguro que se sentirían orgullosos de ver en lo que me he convertido.

A mis amigos de siempre por estar en los momentos de agobio, estudio y celebraciones. Destacar a mi gran amiga Azahara, cuyo ánimo y consejos han sido y serán siempre muy útiles para mi.

Por último agradecer a Paz por compartir su vida conmigo día a día, ofrenciendome su apoyo durante esta etapa tanto en los momentos buenos como en los malos, animándome y dándome fuerzas para seguir adelante.

Sin todos vosotros esto no habría sido posible, muchas gracias.

Resumen

Actualmente, el manejo de información y datos sensibles en la mayoría de empresas y aplicaciones es un tema muy controvertido y preocupante para los usuarios. Vivimos en una época en la que interactuamos con dispositivos móviles y ordenadores constantemente tanto en el ámbito personal como profesional. En ciertos momentos utilizamos aplicaciones en las que confiamos nuestros datos personales, contraseñas, etc., sin preocuparnos o preguntarnos que nivel de seguridad nos pueden ofrecer.

El presente Trabajo de Fin de Grado tiene como objetivo analizar la seguridad e integridad de datos en diferentes ámbitos y proponer un índice de seguridad que, en la medida de lo posible, sirva de herramienta para evaluar la seguridad de los datos a aquellas organizaciones o aplicaciones que traten con información sensible.

Para poder realizar dicho análisis, se comienza por un estudio de las principales normas que existen en la actualidad para diferentes ámbitos de la seguridad. De este modo se analizan las normas ITIL, COBIT, Magerit e ISO. A partir de este estudio, se eligen los ámbitos de la seguridad que se desean analizar y se procede a la elaboración del índice de seguridad.

El índice de seguridad propuesto debe ser medible para facilitar a aquellas personas que deseen utilizarlo, la comprobación del nivel de seguridad en los ámbitos analizados. Como último dato, este índice ofrece información acerca de los indicadores (estos son cada uno de los puntos medibles establecidos en un ámbito) de seguridad con mayor peso (importancia) dentro de la seguridad total de la información.

Para poder establecer los pesos de los distintos indicadores de seguridad se ha optado por el uso del método de decisión multicriterio AHP teniendo en cuenta dos valoraciones distintas (autor y cotutor del presente TFG).

Por último, una vez obtenido el índice de seguridad y cada uno de los pesos de los indicadores que lo forman, se aplica sobre un caso de estudio que evalúa diferentes alternativas para realizar la elección que mejor se adapte a las necesidades deseadas atendiendo al método propuesto.

Palabras clave: seguridad información, integridad de datos, AHP.

Abstract

Currently, information and sensitive data management in most enterprise applications is a controversial issue that concerns to its users. We are living a time in which we interact with mobile devices and computers both personally and professionally. There are times when we use some applications, providing them our personal details and information, without thinking or wondering the level of confidentially they offer.

This final degree project aims to analyze data security and integrity in different areas and propose a security index necessary to ensure confidentiality to those organizations that deal with sensitive information.

In order to perform this analysis, it is begn by a study of some of the rules exiting nowadays for different security areas. In this way, it is going to be made an analysis of ITIL, COBIT, Magerit and ISO. More specifically of this study, thre have been chosen the security areas to be analyzed and proceed with the preparation of the security index.

The proposed security index must be measurable to facilitate those who wish to use it, check the level of security in some analyzed areas. This index provides information and insights about the security indicators (these are each of the measurable points of the areas) with more weight (importance) within the overall information security.

In order to establish the weights of the security indicators proposed, it is going to be used the multicriteria method AHP taking into account two different valuations (autor and cotutor of this work).

Finally, after obtaining the security index and each of the weights for each indicator, the index is applied to a case study to evaluate different alternatives to make the best choice that best fits with the desired needs using the proposed method.

Keywords: information security, data integrity, AHP.

Tabla de contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. Introducción

En este primer capítulo se realiza una breve introducción del presente Trabajo de Fin de Grado. Para ello se expone el problema existente, las motivaciones para llevar a cabo este trabajo, el objetivo perseguido con la realización del mismo y los contenidos que se han desarrollado.

1.1. Problemática y necesidad

Los datos de carácter personal están presentes en el día a día de cualquier persona. Actualmente, la mayoría de las transacciones que involucran datos personales de carácter sensible, se realizan utilizando aplicaciones informáticas o internet. Esto es un gran problema ya que constantemente facilitamos nuestros datos personales para acceder al correo, comprobar cuentas de banco de forma online, acceder a redes sociales, etc. Estos datos podrían verse atacados por terceras personas si no se encuentran protegidos de forma adecuada.

Todas las aplicaciones que tratan con datos sensibles deberían garantizar un mínimo de seguridad y confidencialidad que asegure al usuario que sus datos serán utilizados para fines correctos. Este tipo de aplicaciones deben estar controladas y reguladas legalmente, de tal modo que sus responsables aseguren el correcto funcionamiento y tratamiento de la información, así como la responsabilidad ante una posible mala praxis.

Debido a las amenazas y vulnerabilidades existentes, tales como ataques a dipositivos móviles, suplantación de identidad o robo de información que surgen en torno a la protección de datos sensibles, es necesario controlar de algún modo las aplicaciones que gestionan esta información. Por este motivo se ha creído necesario realizar este trabajo de investigación cuyo objetivo es realizar un análisis del tema y establecer un índice de seguridad que incluya indicadores medibles para garantizar la protección de datos en varios ámbitos de la seguridad.

1.2. Motivación de trabajo

La motivación de este trabajo surge de la curiosidad personal de saber cómo se gestionan los datos sensibles en diferentes ámbitos de la seguridad de la información. Como usuario potencial de internet, se me solicita información de carácter privado a diario, y en ciertos momentos la doy con cierto recelo por no saber de que forma se garantiza que no se hará un uso fraudulento de ella o se revelará a terceros. Del mismo modo, me resulta interesante conocer como se puede medir el nivel de seguridad en las TI existente en una aplicación u organización, ya que en apariencia resulta ser un tema abstracto.

1.3. Objetivo

El presente trabajo propone un índice de seguridad que pretende resolver, en la medida de los posible, las dudas que surgen en cuanto a como medir la seguridad para garantizar la integridad de los datos.

Para ello se analizarán los estándares existentes ITIL, COBIT, MAGERIT e ISO para conocer las ventajas de cada uno de ellos y observar sus principales diferencias.

Como producto final se ofrecerá un índice de seguridad compuesto por varios indicadores medibles y aplicables al tratamiento de datos para poder establecer el nivel de contribución de los diferentes indicadores seleccionados. Para realizar el cálculo de la contribución de los indicadores se utilizará un método de decisión multicriterio.

1.4. Terminología

Dentro de este apartado se explican brevemente algunos de los términos utilizados en el desarrollo del presente trabajo para que el lector pueda comprender mejor su contenido. Del mismo modo se explicará el significado de todos los acrónimos recogidos en el documento.

1.4.1. Glosario de términos

A continuación se definen algunos de los términos utilizados en el trabajo que pueden no quedar suficientemente claros en el desarrollo del mismo. El significado de cada término es el siguiente:

- **Stakeholders:** todas aquellas personas o entidades que pueden afectar o son afectados por las actividades de una empresa.
- **Indicador:** cada uno de los elementos establecidos en el índice de seguridad propuesto.
- **Ámbito de seguridad:** división elegida dentro de las áreas existentes de la seguridad informática.
- **Sub-ámbito de seguridad:** subdivisión realizada dentro de un ámbito de seguridad.
- **Peso o contribución:** nivel aportado por un indicador, ámbito o sub-ámbito al índice de seguridad calculado mediante el método AHP.

1.4.2. Acrónimos

El significado de los acrónimos utilizados en el presente trabajo es el siguiente:

- **TI:** Tecnologías de la información
- **ITIL:** Information Technology Infrastructure Library
- **COBIT:** Control Objectives for Information and related Technology
- **MAGERIT:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- **CSAE:** Consejo Superior de Administración Electrónica
- **ISO:** International Organization of Standarization
- **IEC:** International Electrotechnical Commission
- **NASA:** National Aeronautics and Space Administration
- **IBM:** International Business Machines
- **HP:** Hewlett Packard
- **UK:** United Kindom
- **HSBC:** The Hong Kong and Shanghai Banking Corporation
- **ISACA:** Information Systems Audit and Control Association
- **IVA:** Impuesto sobre el Valor Añadido
- **SGSI:** Sistema de Gestión de la Seguridad de la Información
- **AHP:** Analytic Hierarchy Process
- **MAUT:** Multi-Attribute Utility Theory
- **ELECTRE:** Elimination Et (and) Chhoice Translating Algorithm
- **PROMETE:** Preference Ranking Organization Method for Enrichement Evaluations
- **TIC:** Tecnologías de la Información y Comunicación
- **CCMv3:** Cloud Control Matrix Version 3
- **VMM:** Virtual Machine Monitor
- **MIT:** Massachusetts Institute of Technology
- **ICT:** Information and Communication Technology

1.5. Contenido de la memoria

A continuación se realiza un breve resumen de los temas indicados en el índice de contenidos del documento:

- **Introducción:** en este apartado se presenta el tema tratado en el presente Trabajo de Fin de Grado. Para ello se analizan el problema que se pretende solventar, la necesidad de análisis del tema y el objetivo perseguido. Además incluye un apartado de terminología en el que se detalla un glosario de términos y acrónimos.
- **Estado del arte:** en este apartado se analizan las metodologías existentes hoy en día que guardan relación con el tema propuesto en el TFG. Para ello se realiza un estudio de los métodos ITIL, COBIT, MAGERIT e ISO.
- **Análisis de indicadores de seguridad:** dentro de este apartado se incluye la selección de los ámbitos y sub-ámbitos elegidos para realizar el índice de seguridad.
- **Priorización de indicadores de seguridad:** dentro de este apartado se definen cada uno de los indicadores propuestos para cada ámbito. Además se ofrece una breve explicación y medida de cada uno de ellos.
- **Priorización de indicadores de seguridad:** una vez establecido el índice de seguridad y seleccionados los indicadores, en este apartado se procede a obtener el valor de cada indicador (su peso o contribución al índice). Para ello se analizan los métodos de decisión multicriterio Scoring, MAUT, Relaciones de sobreclasificación y AHP. Finalmente se elige el método AHP, se ejecuta y se obtienen y analizan los resultados que ofrece.
- **Caso de estudio:** una vez obtenido el índice de seguridad, se tienen los diferentes valores para los elementos involucrados, por lo tanto se aplica el índice de seguridad sobre un caso de estudio para la elección de la alternativa acorde a la metodología propuesta.
- **Conclusiones y trabajo futuro:** en este apartado se incluyen una serie de comentarios finales al trabajo realizado así como un línea de trabajo futuro.
- **Planificación y presupuesto:** este apartado contiene la planificación del presente Trabajo de Fin de Grado así como el presupuesto del mismo.
- **ANEXO A:** en este apartado se incluye una versión extendida correspondiente al resumen en inglés del presente Trabajo de Fin de Grado.

2. Estado del arte

En este apartado se contemplan algunas de las metodologías existentes en el ámbito de la gestión de servicios de TI. Se presta especial atención a cómo cada uno de estos métodos contribuye en la gestión de la seguridad de datos.

Partiendo del análisis de los diferentes métodos existentes y teniendo en cuenta la divergencia entre ellos para un área crítica como la seguridad, el objetivo es aunar el esfuerzo realizado en iniciativas previas y crear un modelo de indicadores (índice de seguridad) para medir sistemáticamente la seguridad en los sitemas de TI.

2.1. ITIL[1]

2.1.1. ¿Qué es?

La Biblioteca de Infraestructura de Tecnologías de Información, en inglés ITIL, es una recopilación de conocimientos y prácticas para la gestión de servicios, desarrollo y operaciones llevadas a cabo con las tecnologías de la información. ITIL propone un conjunto de procedimientos de gestión pensados para ayudar a las organizaciones a lograr mayor calidad y eficiencia en las operaciones de TI. Estos procesos han sido desarrollados como una guía que abarca toda infraestructura, desarrollo y operaciones de TI.

El fin último de ITIL es abogar para que los servicios de TI estén alineados con las necesidades de negocio y apoyen sus procesos centrales. Además, proporciona orientación, tanto a organizaciones como individuos particulares, sobre el uso de las TI en la transformación y crecimiento de negocios.

La Biblioteca ITIL fue desarrollada en 1980 y posteriormente revisada y ampliada a mediados de los años 90. Esta última revisión ha incluido varios estándares, entre ellos la norma internacional ISO/IEC/20000 de gestión de servicios TI. ITIL se relaciona con la gobernanza de tecnologías de la información mediante COBIT.

ISO/IEC/20000 e ITIL son totalmente compatibles entre ellas. La ventaja que presenta ISO/IEC/20000 frente a ITIL es su mayor facilidad para ser medible dentro de un proceso de auditoría. La gestión de servicio realizada por ITIL está actualmente integrada en el estándar ISO 20000 (anteriormente BS 15000).

1 *AXELOS* 26/02/2015 <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>

ITIL se detalla en una serie de publicaciones, cada una de ellas dirigida a un ámbito en concreto dentro de la gestión de TI. La última revisión de ITIL ha dado lugar a un nuevo conjunto de publicaciones denominados como ITIL versión 3. Los diferentes ámbitos tratados en las publicaciones son los siguientes:

- Estrategia de servicios
- Diseño de servicios
- Transacción de servicios
- Operación de servicios
- Mejora continua de servicios

La administración de los servicios de TI está directamente relacionada con la mejora de los procesos mediante el uso de tecnologías y su integración con los usuarios. Esto precisamente está muy relacionado con ITIL ya que es necesario conseguir un cierto equilibrio entre procesos, tecnología y usuarios.

Figura 1: Integración de personas, procesos y tecnologías[2]

En la Figura 1 puede observarse la relación que se establece dentro de la administración de servicios de TI entre los procesos, la tecnología y las personas.

ITIL es utilizado tanto a nivel particular como a nivel de grandes organizaciones para llevar a cabo la gestión de los servicios de TI.

2 *Administración de servicios de TI* 26/02/2015 <http://www.magazcitum.com.mx/?p=50>

Dentro de los usuarios potenciales de ITIL destacan los siguientes:

- NASA
- Microsoft
- IBM
- HP
- Shell
- Procter&Gamble
- UK National Health Service
- HSBC

2.1.2. ¿Qué certificaciones ofrece?[3]

El Esquema de Certificación ITIL propone una serie de certificaciones dirigidas a diferentes ámbitos de las buenas prácticas de ITIL con diversos grados de profundidad y detalle. La estructura de niveles de calificación ofrece a los usuarios cierta flexibilidad en relación con las diferentes disciplinas y áreas de ITIL. Dentro del esquema de certificación existen cuatro niveles cada uno de ellos con unas características en concreto. Las certificaciones ofrecidas por ITIL pueden observarse en la Tabla 1.

NIVEL	CARACTERÍSTICAS
Fundación	Nivel de entrada que ofrece un conocimiento general de los elementos clave, conceptos y terminología utilizados en el ciclo de vida del servicio de ITIL. Incluye los vínculos entre las etapas del ciclo de vida, los procesos utilizados y su contribución a la gestión de servicios.
Intermedio	Este nivel tiene una estructura modular en la que cada módulo se focaliza en un área diferente de la gestión de servicios TI. Pueden obtenerse tantos módulos del nivel intermedio como sean necesarios.
Experto	Este nivel de certificación está orientado a aquellos que estén interesados en demostrar el conocimiento del esquema ITIL en su totalidad.
Master	Para conseguir esta certificación se debe ser capaz de explicar la selección y aplicación de una serie de conocimientos, principios, métodos y técnicas de ITIL y las técnicas de gestión que lo justifique para lograr los resultados de negocio deseados.

Tabla 1: Niveles de certificación de ITIL

3 *QRPInternational* 26/02/2015 <http://www.qrpinternational.es/index/itil/what-is-itil>

La jerarquía establecida en los diferentes niveles de certificación de ITIL puede observarse en la Figura 2.

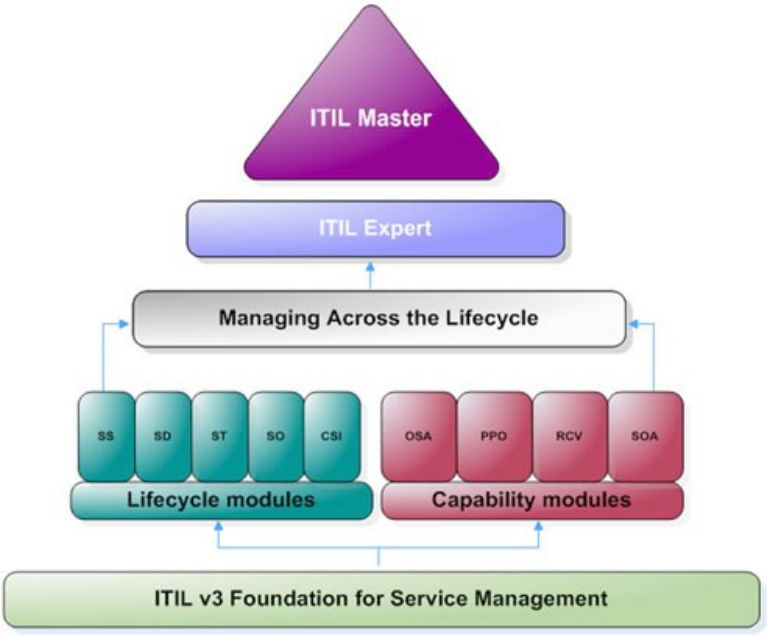


Figura 2: Jerarquía niveles de certificación ITIL[4]

2.1.3. ITIL y la integridad de datos[5]

ITIL colabora directamente con la gestión de la seguridad en el establecimiento de políticas y planes de seguridad. Esto es necesario para minimizar los daños en caso de producirse un problema.

Dentro de la Gestión de la Seguridad es de vital importancia que se den las siguientes condiciones:

- Todo personal que utiliza los recursos conoce y acepta tanto las medidas de seguridad como sus responsabilidades respecto a los recursos.
- Existen acuerdos de confidencialidad para los empleados.
- Todos los empleados son conocedores de las conductas esperadas de ellos. En algunos casos será necesario impartir la formación necesaria.

4 *Ruta de certificación ITIL* 26/02/2015 <http://www.blauconsulting.com/itil/mapa-de-certificacion-itil.html>

5 *ITIL – Gestión de servicios de TI* 26/02/2015 <http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/proceso_gestion_de_la_seguridad/aplicacion_medidas_de_seguridad.php>

Dentro de la Gestión de la Seguridad se debe asegurar el cumplimiento y verificación de los siguientes aspectos:

- Proporcionar la documentación necesaria durante todo el proceso de Gestión de Seguridad.
- Proporcionar los recursos necesarios.
- Gestión de incidentes y tratamiento de soluciones.
- Gestión de cambios y versiones.
- Gestión de la continuidad y servicio de forma que se garantice la **integridad y confidencialidad** de los datos.
- Mantenimiento de hardware y software actualizado.
- Establecimiento de políticas y protocolos de acceso a la información.

El cumplimiento de lo expuesto anteriormente resultará en un producto con calidad suficiente como para llevar a cabo una correcta gestión de seguridad. Sin embargo, atendiendo al objetivo del presente Trabajo de Fin de Grado se puede observar que la integridad de datos no queda totalmente cubierta puesto que se incluye dentro de otro aspecto en lugar de tratarse de forma individual para explotar todo su contenido.

2.2. COBIT

2.2.1. ¿Qué es?[6]

COBIT es el marco aceptado internacionalmente como una buena práctica para el control y mantenimiento de la información en las TI y los riesgos asociados. Mediante COBIT es posible evaluar la capacidad de los sistemas para generar información pertinente y confiable para la consecución de los objetivos establecidos en una organización.

COBIT establece un modelo con el que se evalúan los siguientes aspectos:

- Procesos involucrados en la organización.
- Recursos que comprenden las TI dentro de la organización.
- Criterios de información.

La última versión de COBIT (COBIT 5) fue lanzada en Abril de 2012. Está basada en la versión anterior (COBIT 4.1) y a su vez lo amplía mediante la integración de otros marcos y normas entre los que destacan las normas ISO e ITIL. La versión COBIT 4.1 (disponible desde 2007) cubre una serie de objetivos de control que se clasifican en cuatro áreas de domino:

1. Planificación y Organización
2. Adquisición e Implantación
3. Entrega y Soporte
4. Supervisión y Evaluación

6 *Turevisorfiscal* 28/02/2015 <http://turevisorfiscal.com/que-es-el-cobit/>

Cada una de estas áreas está destinada a controlar una parte de las TI dentro de una organización mediante el análisis de objetivos predefinidos.

2.2.2. ¿A quién está dirigido?

Dentro de una organización existen diferentes grupos de usuarios. COBIT proporciona beneficios a casi la totalidad de ellos. La aplicación de COBIT en una organización está dirigida a los siguientes grupos:

- **Auditores:** sus decisiones estarán basadas y apoyadas en el modelo COBIT. Mediante la utilización de este método podrán establecer los requisitos mínimos para el cumplimiento de los objetivos de la organización.
- **Gerencia:** reforzarán las decisiones tomadas por éstos sobre las inversiones en TI y su gestión.
- **Usuarios finales:** obtienen una garantía sobre los productos finales obtenidos.

2.2.3. ¿Qué certificaciones ofrece?[7]

Dentro de la última versión de COBIT (COBIT 5) editada por ISACA, se establecen tres niveles en los que poder especializarse, garantizando cada uno de ellos una serie de conocimientos sobre este método. Los niveles establecidos pueden comprobarse en la Tabla 2.

NIVEL	CARACTERÍSTICAS
Fundación	Este nivel proporciona conocimientos suficientes como para entender las gobernanzas de la TI, crear conciencia con otros miembros de la organización, evaluar el estado de la empresa en un departamento en concreto y determinar que aspectos de COBIT 5 se deberían implementar.
Implementación	Proporciona un entendimiento práctico de cómo aplicar COBIT 5 a problemas específicos de la empresa, puntos débiles y riesgos dentro de la organización.
Asesor	Este nivel proporciona métodos para ayudar a la implementación de procesos. Se proporcionará el conocimiento suficiente para realizar evaluaciones de procesos y análisis de sus resultados. También se obtendrá el conocimiento necesario para conocer que áreas de los procesos deben ser mejoradas y métricas para la consecución de objeticos.

Tabla 2: Niveles de certificación COBIT

7 *COBIT5 Qualifications* 28/02/2015 <http://www.apmginternational.com/en/qualifications/cobit5/cobit5.aspx>

2.2.4. COBIT y la integridad de datos[8]

La última versión de COBIT (COBIT 5) persigue la creación de una guía práctica para garantizar la seguridad en la organización. Dentro del ámbito de la seguridad de la información e integridad de datos, COBIT puede reducir los riesgos existentes a través de su correcta administración.

Además, entre los objetivos principales de COBIT en el establecimiento de una guía práctica de las TI, destacan los siguientes:

- Garantizar la confidencialidad, integridad y disponibilidad de los datos e información.
- Asegurar la correcta gobernanza de las TI, protegiendo en todo momento los intereses de los *stakeholders*.
- Garantizar el cumplimiento de las normas existentes en los ámbitos organizacionales.
- Mejorar la eficacia y eficiencia de los procesos y actividades de la organización.

La guía de mejores prácticas presentada por COBIT tiene en cuenta de forma individual entre sus objetivos la integridad de los datos. Sin embargo esta norma no propone ningún tipo de medida con la que cuantificar el nivel de integridad y confidencialidad de los datos e información.

2.3. MAGERIT[9]

2.3.1. ¿Qué es Magerit?

Magerit es una metodología de análisis y gestión de riesgos de los Sistemas de la Información elaborada por el CSAE para minimizar los riesgos de la implantación y uso de las TI enfocada a la Administración Pública. Esta metodología incumbe tanto a la información digitalizada como a los sistemas informáticos para tratarla.

El uso de TIC supone grandes beneficios para los ciudadanos pero también da lugar a riesgos que deben gestionarse con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

La metodología Magerit persigue una aproximación metódica al problema que surge al analizar dichos riesgos. Los objetivos de Magerit son los siguientes:

8 *Estándar para el buen gobierno de los sistemas de la información* 28/02/2015 <http://www.marblestation.com/?p=645>

9 *Metodología de análisis y gestión de riesgos de los Sistemas de Información* 02/03/2015<http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VU4kCtPtmko>

- Dar conocimiento de la existencia de riesgos y la necesidad de minimizar sus efectos a los responsables de los sistemas de información.
- Proponer un método sistemático para analizar los riesgos.
- Planificar las medidas y planes de contingencia para los riesgos.
- Preparación para procesos de evaluación de la organización: auditoría, certificación o acreditación.

El funcionamiento del método Magerit puede observarse en la Figura 3.

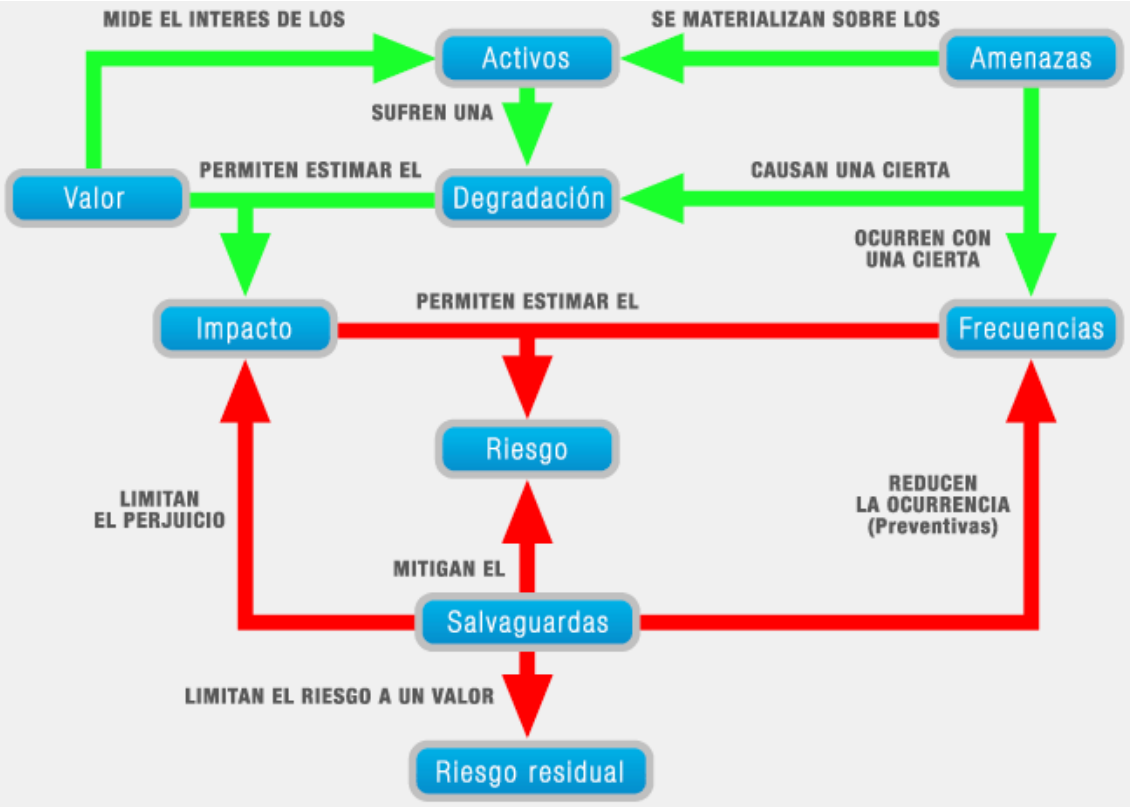


Figura 3: Funcionamiento metodología Magerit[10]

2.3.2. Estructura de la metodología[11]

La estructura de Magerit se desarrolla en tres submodelos:

- Elementos: proporciona los componentes del sistema (activos, amenazas, vulnerabilidades, impacto, riesgo y salvaguarda).
- Eventos: relaciona los elementos entre si y con el tiempo.
- Procesos: describe el proceso de seguridad en cuatro etapas (planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas).

10 *Funcionamiento metodología Magerit* 02/03/2015 <https://www.ccn-cert.cni.es/publico/herramientas/pilar-5.3.1/>

11 *Metodología de análisis y gestión de riesgos de los Sistemas de Información* 02/03/2015 <https://seguridadinformaticaufps.wikispaces.com/MAGERIT>

La versión 2 de Magerit se ha estructurado en tres libros:

- **El método:** en este libro se exponen los pasos para realizar un análisis de los riesgos así como el establecimiento de los planes de mitigación. Se describen también las tareas básicas de cómo realizar un proyecto de análisis y gestión de riesgos. Más adelante se aplica la metodología al caso de desarrollo de sistemas de información. Por último se ofrecen una serie de consejos prácticos adquiridos mediante la experiencia.
- **Catálogo de elementos:** este libro ofrece un catálogo en cuanto a tipos de activos, dimensiones y criterios de valoración de los mismos, amenazas más comunes sobre los sistemas de información y salvaguardas para proteger los sistemas de información. Este libro persigue, por una parte facilitar la labor de las personas que realizan el proyecto, y por otra homogeneizar los resultados de los análisis.
- **Guía de técnicas:** este libro ofrece una serie de técnicas que se llevan a cabo durante los procesos de análisis y gestión de riesgos tales como técnicas de análisis, análisis mediante tablas, diagramas de flujo, técnicas gráficas, etc.

En el caso del método MAGERIT no cubre de forma extensa el ámbito de la integridad de datos puesto que sólo evalúa la misma atendiendo a los riesgos que puedan aparecer. Para cubrir la integridad y confidencialidad de los datos de forma completa es necesario tener en cuenta como se gestionan internamente los mismos.

2.4. ISO[12]

2.4.1. ¿Qué es?

La Organización Internacional para la Estandarización (ISO) es una organización a nivel mundial que integra diferentes cuerpos de estandarización de varios países. Su finalidad es la creación y promoción de normas internacionales que cubran la mayor parte de ámbitos empresariales. Su función principal es la estandarización de normas a nivel internacional relativas a productos y seguridad de las empresas.

2.4.2. ISO/IEC y la integridad de datos[13]

La seguridad de la información e integridad de datos está controlada por la serie 27000 de los estándares ISO/IEC. En términos generales esta norma trata de:

- Preservar la confidencialidad de los datos de la organización
- Garantizar la integridad de los datos de la organización
- Garantizar la disponibilidad de toda la información existente

12 *ISO Standards* 01/03/2015 <http://www.iso.org/iso/home/standards.htm>
13 *La serie ISO27000* 01/03/2015 <http://www.iso27000.es/download/doc_iso27000_all.pdf>

Dentro de esta serie existen una serie de normas enfocadas a la gestión de la seguridad. Atendiendo a la motivación de este Trabajo de Fin de Grado, dentro de esta serie se va a analizar las normas: ISO-27000, ISO-27001, ISO-27002, ISO-27003 e ISO-27004.

2.4.3. ISO 27000

Esta norma contiene los términos y definiciones que se emplearan en toda la serie 27000. Esta norma se utiliza para tener un entendimiento más claro y una visión global de los diferentes documentos que la forman. Hace hincapié en la necesidad de que los términos se utilicen de forma consistente y coherente durante toda la norma.

2.4.4. ISO 27001

La norma ISO/IEC 27001 es un estándar para la seguridad de la información aprobada y publicada en 2005 y posteriormente revisada en 2013. Describe como gestionar la seguridad de la información en una organización proporcionando una metodología de implementación.

El SGSI que propone esta norma se puede resumir en las fases que se muestran en la Figura 4.

Figura 4: Fases SGSI ISO 27001[14]

Esta norma ofrece una serie de ventajas entre las que destacan las siguientes:

- Identifica los riesgos estableciendo una serie de controles para llevar a cabo su gestión o eliminación
- Flexibilidad de adaptación de controles total o parcial
- Confianza frente a la protección de datos

14 *ISO 27001: Gestión de la Seguridad de la Inforamción* 02/03/2015 <http://www.normas-iso.com/iso-27001>

La ISO 27001 propone 11 dominios con 39 objetivos de seguridad desgranados en 133 controles para la gestión de la seguridad. Cada uno de estos controles pretende garantizar que cada riesgo evaluado quede cubierto y sea auditable para poder llevar a cabo un registro.

Los controles que propone esta norma quedan agrupados en los siguientes grupos:

- Política de seguridad
- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones
- Control de accesos
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Administración de los incidentes de seguridad
- Administración de la continuidad de negocio
- Cumplimiento (legales, de estándares, técnicas y auditorías)

Dentro de cada uno de estos grupos (objetivos) se proponen una serie de controles hasta completar los 133 propuestos en esta norma.

Atendiendo a la naturaleza, estructura y objetivo de esta norma, se puede relacionar directamente con el objetivo del presente Trabajo de Fin de Grado en el que se persigue establecer un índice de seguridad en el que se definan una serie de métricas (indicadores) verificables para cuantificar el nivel de seguridad de una organización. Por este motivo, esta norma se ha tomado como referencia para el establecimiento y selección de cada uno de los indicadores que se proponen más adelante en el índice de seguridad.

2.4.5. ISO 27002

La norma ISO/IEC 27002 es una guía de buenas prácticas en la que se describen los principales objetivos de control de la seguridad de la información. Dentro de este estándar la seguridad de la información se define como “capacidad de preservar la confidencialidad, integridad y disponibilidad de la información”. La última actualización de esta normal data del año 2013, en la que se establecían una serie de dominios principales entre los que destacan la organización de la seguridad de la información, el control de accesos, la seguridad física y la gestión de incidencias entre otros.

Dentro de cada sección se establecen una serie de objetivos establecidos para garantizar la seguridad de la información. Esta norma es sólo una guía de prácticas que en ningún caso establece unos requisitos de certificación verificables que garanticen la obtención de esta norma.

2.4.6. ISO 27003

La norma ISO/IEC 27003 es la guía de implantación de un SGSI. Esta norma tiene como objetivo principal garantizar el éxito del diseño e implementación de un SGSI. En esta norma se especifica desde el diseño inicial hasta la forma en que se ha de llevar a cabo su ejecución. Esta norma se complementa directamente con la ISO/IEC 27001 y al igual que la norma ISO/IEC 27002 no establece requisitos de certificación.

2.4.7. ISO 27004[15]

La norma ISO/IEC 27004 tiene como objetivo medir el resultado de un SGSI basado en la norma ISO/IEC 27001. Esta normal define el tipo de medición, que parámetros son necesarios medir y como realizar dicha medición.

Los resultados que arrojan las mediciones de la seguridad son muy importantes ya que pueden dejar entrever los puntos más débiles de una organización y por lo tanto es más fácil establecer estrategias para minimizar las amenazas ante estos riesgos. Las fases propuestas por la norma ISO/IEC 27004 para medir la seguridad de la información son las siguientes:

- Selección de procesos y objetos de medición
- Definición de las líneas base
- Recopilación de datos
- Desarrollo del método de medición
- Interpretación de resultados
- Comunicación de resultados

La familia de normas ISO-27000 es la que mejor cubre la integridad de datos dentro de un proceso de medición de seguridad en una organización. Más concretamente la norma ISO-27001 es la que propone una serie de controles para verificar la seguridad. Sin embargo la norma muestra un carácter muy amplio y es por eso por lo que en este trabajo se propone un índice enfocado exclusivamente a ciertas áreas de la seguridad de los datos. Además en algunos casos los objetivos no pueden ser cuantificados de una forma sencilla que es, por otro lado, lo perseguido en este trabajo.

15 *Medición de la Seguridad de la Información* 03/03/2015 <http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/>

3. Análisis de indicadores de seguridad[16]

Tras el análisis de la seguridad e integridad de los datos en los métodos existentes realizado en el apartado anterior, se persigue encontrar una serie de indicadores de seguridad que sean fácilmente medibles para la elaboración de un índice de seguridad. Se trata de encontrar un modelo que facilite a una organización conocer el grado de seguridad que puede ofrecer a sus clientes en los ámbitos de seguridad seleccionados.

A partir de los métodos analizados, se van a proponer una lista de indicadores medibles para cubrir tres ámbitos de la seguridad de la información.

Los ámbitos elegidos para la realización del índice de seguridad son los siguientes:

- Acceso y privilegio
- Entorno físico
- Integridad de datos

Para cada uno de estos ámbitos, se ha realizado una división en sub-ámbitos teniendo en cuenta la relación entre los indicadores de cada uno de ellos para su correcta clasificación.

Como se indicó anteriormente, para el establecimiento de éste índice de seguridad se ha tomado como referencia la norma ISO 27001. A partir de un análisis de sus objetivos y controles, se han seleccionado los diferentes ámbitos de seguridad para la clasificación de los indicadores de seguridad que se evalúan en el presente trabajo.

Además para la realización de este apartado se ha tomado como base la matriz "Cloud Controls Matrix Version 3.0" (CCMv3) en la que existe una división en ámbitos de seguridad y dentro de cada uno de ellos una serie de indicadores. A partir de esta matriz y de los métodos analizados anteriormente (principalmente ISO 27001) se ha hecho la división y determinación de los indicadores de seguridad.

A continuación se listan los diferentes ámbitos y sub-ámbitos seleccionados para la realización del índice de seguridad, aunque donde yace la importancia de este trabajo es en la contribución a la medida de cada indicador propuesto para dichos ámbitos y sub-ámbitos.

16 *Cloud Controls Matrix Version 3* 10/03/2015 <https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx>

3.1. ACCESO Y PRIVILEGIO

Dentro de este ámbito se encuentran aquellos indicadores relacionados principalmente con el manejo de la información por parte de los diferentes usuarios, desde su acceso a las plataformas, permisos que tienen o infraestructuras que utilizan. A su vez, dentro de este ámbito se ha subdivido en sub-ámbitos para catalogar de una forma mejor cada uno de los indicadores.

3.1.1. Seguridad y recursos humanos

- Requisitos de acceso
- Identificación de equipamiento
- Administración de dispositivos móviles
- Roles/Responsabilidades
- Espacio de trabajo

3.1.2. Administración de identidad y acceso

- Herramientas de auditoría de acceso
- Ciclo de vida de credenciales/Administración de privilegios
- Políticas y procedimientos
- Segregación de funciones
- Restricciones de acceso al código fuente
- Acceso de terceros
- Fuentes confiables
- Autorización de acceso de usuarios

3.1.3. Infraestructura y seguridad virtual

- Auditoría de acceso/Detección de intrusos
- Seguridad en la red
- Segmentación
- Seguridad VMM
- Seguridad inalámbrica
- Contraseñas

3.2. ENTORNO FÍSICO

El ámbito de entorno físico abarca todos aquellos indicadores que hacen referencia al escenario en que se localizan físicamente los datos con los que se está trabajando. Dentro de este ámbito, del mismo modo que con los anteriores, se ha realizado una nueva subdivisión para clasificar de una forma más exacta los indicadores propuestos.

3.2.1. Gestión de negocios de la continuidad

- Servicios de centros de datos
- Riesgos medioambientales
- Localización del equipamiento

3.2.2. Gestión del centro de datos

- Políticas
- Autorización de área de seguridad
- Entrada no segura

3.2.3. Gestión de acceso

- Puntos de control de acceso
- Acceso de usuarios
- Entrada no autorizada

3.3. INTEGRIDAD DE DATOS

Dentro de este ámbito se engloban los indicadores que hacen referencia a los datos directamente, desde su almacenamiento, encriptado o seguridad virtual de los mismos. Dentro de este ámbito se ha hecho una sub-clasificación para que cada grupo de indicadores quede mejor definido.

3.3.1. Seguridad de datos y administración del ciclo de vida de la información

- Integridad de datos
- Clasificación
- Política de seguridad
- Fuga de información
- Propiedad/Administración
- E-commerce (Comercio electrónico)

3.3.2. Cifrado y gestión de claves

- Generación de claves
- Protección de datos sensibles
- Almacenamiento y acceso

3.3.3. Seguridad virtual y móvil

- Seguridad/Protección de datos
- Cifrado
- Almacenamiento de datos seguros en la nube

4. Diseño de un índice de seguridad[17]

En este apartado definen cada uno de los indicadores propuestos en el apartado anterior. Además, para cada uno de ellos se propone una medida sencilla que facilite los cálculo a aquellos que deseen utilizar este método para evaluar diferentes alternativas en cuanto a seguridad de datos.

Para la realización de este apartado, de nuevo se ha prestado especial interés a la matriz CCMv3 y la norma ISO 27001 del mismo modo que se indicó en los apartados anteriores.

A continuación se incluye una tabla tipo para indicar el formato en el que se listan cada uno de los indicadores.

ÁMBITO				
TIPO	ID	INDICADOR	DEFINICIÓN	MÉTRICA

Tabla 3: Formato tabla indicadores

Atendiendo a la Tabla 3, se puede comprobar que para cada ámbito de la seguridad analizado existe una tabla. Dentro de esta tabla encontraremos los siguientes atributos:

- **Tipo:** cada uno de los grupos en los que se dividen los diferentes ámbitos de seguridad.
- **ID:** identificador de cada indicador dentro de su ámbito. Normalmente se compone de las siglas de su tipo y un número correlativo.
- **Indicador:** nombre del indicador.
- **Definición:** explicación del indicador.
- **Métrica:** fórmula para realizar el cálculo de dicho indicador.

4.1. Acceso y privilegio[18,19]

A continuación describen cada uno de los indicadores elegidos para el ámbito “Acceso y privilegio” así como la medida propuesta para cada uno de ellos. Estos indicadores se definen en la Tabla 4.

17 *Matriz de controles Version 3* 10/03/2015 <https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx>
18 *Control de acceso a la información* 18/03/2015 <http://www.ongei.gob.pe/publica/metodologias/lib5007/313.HTM>
19 *Control de acceso* 18/03/2015 <http://www.alapsi.net/images/Capsula_1_de_4_ca.pdf>

ACCESO Y PRIVILEGIO				
Seguridad y recursos humanos	SRHH-01	Requisitos de acceso	Prioridad para garantizar el acceso de los clientes a datos, activos y sistemas de la información de forma segura	Número de accesos seguros/Número total de accesos
	SRHH-02	Identificación de equipamiento	La identificación automatizada de equipamiento se deberá utilizar como método de autenticación de la conexión. Las tecnologías de reconocimiento de ubicación pueden ser utilizadas para validar la integridad de autenticación de la conexión basada en ubicación conocida de equipamiento	Número de conexiones autenticadas/Número total de conexiones
	SRHH-03	Administración de dispositivos móviles	Las políticas y los procedimientos serán establecidos, y el apoyo a los procesos de negocio y las medidas técnicas serán implementadas para gestionar los riesgos de negocio asociados al uso de dispositivos móviles para el acceso a los recursos corporativos de forma segura	Numero de móviles securizados/Número total de móviles
	SRHH-04	Roles/ responsabilidades	Los roles y responsabilidades de los empleados deberán estar documentados en lo que respecta a la seguridad de la información y activos	Número de roles documentados/Número total de roles
	SRHH-05	Espacio de trabajo	Las políticas y los procedimientos serán establecidos para requerir que los espacios de trabajo sin supervisión no tengan visibilidad abierta de documentos sensibles y que las sesiones de usuarios que hayan estado inactivas un cierto tiempo sean inhabilitadas	Número de espacios de trabajo supervisados/Número total de espacios de trabajo

Administración de identidad y acceso	AIA-01	Herramientas de auditoría de acceso	El acceso y uso de herramientas para auditar los sistemas de información de la organización deben ser segmentados apropiadamente y restringidos para evitar el compromiso y el mal uso de los datos de acceso	Número de herramientas con acceso restringido/Número total de herramientas
	AIA-02	Ciclo de vida de credenciales/ Administración de privilegios	Las políticas de uso y acceso serán establecidas y el apoyo a los procesos de negocio y las medidas técnicas serán implementadas para asegurar la identidad apropiada, el derecho y la gestión de acceso para todos los usuarios internos con acceso a los datos de aplicaciones	Número de credenciales activas/Número total de credenciales
	AIA-03	Políticas y procedimientos	Las políticas y procedimientos se establecerán para almacenar y gestionar la información de identidad sobre cada persona que accede a la infraestructura de TI y para determinar su nivel de acceso. Las políticas también deben ser desarrolladas para controlar el acceso a los recursos de red basados en la identidad del usuario	Número de personas con políticas establecidas/Número total de personas
	AIA-04	Segregación de funciones	Las políticas y procedimientos de acceso de usuario deben ser establecidas y el apoyo a los procesos de negocio y las medidas técnicas deben ser implementadas para restringir el acceso de los usuarios según la segregación de tareas	Número de accesos restringidos/Número total de accesos
	AIA-05	Restricciones de acceso al código fuente	El acceso a aplicaciones propias de la organización, programas, código fuente objeto o cualquier otra forma de propiedad intelectual, y el uso de software propietario	Número de accesos al código fuente restringidos /Número total de accesos al código fuente

			debe estar restringido siguiendo la regla del menor privilegio basado en la función de trabajo establecida por acceso y procedimiento de usuario	
	AIA-06	Acceso de terceros	La identificación, evaluación y priorización de los riesgos que plantean los procesos de negocio que requieren el acceso de terceros a los sistemas y datos de información de la organización deberán ir seguidos de la aplicación coordinada de recursos para minimizar, monitorizar y medir la probabilidad y el impacto de acceso no autorizado o inapropiado. Los controles de compensación derivados del análisis de riesgos se aplicarán antes de la provisión de acceso	Número de riesgos encontrados debido a accesos/Número total de accesos
	AIA-07	Fuentes confiables	Las políticas y procedimientos establecidas para el almacenamiento permisible y el acceso de las identidades utilizadas para garantizar la identificación, son sólo accesibles basándose en la norma de menos privilegio y la limitación de usuarios explícitos	Número de fuentes confiables/Número total de fuentes
	AIA-08	Autorización de acceso de usuarios	El aprovisionamiento a los usuarios de acceso a datos y aplicaciones y sistemas de infraestructuras debe ser autorizado por la gestión de la organización para priorizar el acceso garantizado y restringido según las políticas y procedimientos	Número de accesos autorizados/Número total de accesos
Infraestructura y seguridad virtual	ISV-01	Auditoría de acceso/Detección de	Se requieren mayores niveles de garantía para la protección, la conservación y la gestión de	Número de auditorias no superadas/Número total

		intrusos	ciclo de vida de los registros de auditoría, la adhesión a las obligaciones de cumplimiento legal o reglamentos aplicables. Se debe proporcionar una única cuenta de acceso para detectar comportamientos sospechosos o anomalías de integridad y para poder investigar en caso de fallo de seguridad	de auditorias
	ISV-02	Seguridad en la red	Los entornos de red e instancias virtuales deben estar diseñados y configurados para restringir y controlar el tráfico entre conexiones con el apoyo de documentación para el uso de servicios, protocolos y puertos permitidos. Los diagramas de arquitectura de red deben identificar claramente los entornos de alto riesgo y los flujos de datos que pueden tener impactos legales. Se deben aplicar medidas técnicas para la detección de ataques basados en red.	Número de conexiones de red restringidas/Número total de conexiones de red
	ISV-03	Segmentación	La propiedad o gestión de aplicaciones y los sistemas de infraestructuras y componentes de red deben estar diseñados, desarrollados, implementados y configurados de modo que proveedor y cliente tengan un acceso segmentado diferenciado del resto de clientes. Se ha de tener en cuenta lo siguiente: - Políticas y procedimientos establecidos - Aislamiento de los activos críticos de negocio y/o datos de usuario sensibles y sesiones que demandan fuertes	Número de accesos “proveedor”/Número total de accesos ——— Número de accesos “clientes”/Número total de accesos

			controles internos y altos niveles de garantía - Cumplimiento legal	
	ISV-04	Seguridad VMM	El acceso a todas las funciones de gestión de hipervisor o consolas de administración para sistemas de hosting virtualizado deben estar restringidos teniendo en cuenta el principio de menor privilegio y apoyado mediante controles técnicos	Número de accesos VMM seguros/Número total de accesos
	ISV-05	Seguridad inalámbrica	Las políticas y los procedimientos serán establecidas y el apoyo a los procesos de negocio y las medidas técnicas serán implementadas para proteger los entornos de red inalámbrica incluyendo los siguientes: - Firewalls perimetrales implementados y configurados para restringir el tráfico no autorizado - Ajustes de seguridad habilitados para autenticación y transmisión - Acceso de usuario a dispositivos de red inalámbrica restringidos a personal no autorizado - Capacidad para detectar la presencia de dispositivos de red inalámbrica no autorizados	Número de accesos inalámbricos seguros/Número total de accesos inalámbricos
	ISV-06	Contraseñas	Las políticas de contraseña aplicables a dispositivos móviles deberán ser documentadas y se endurecerán mediante controles técnicos en todos los dispositivos y se	Número de dispositivos móviles con contraseña/Número total de dispositivos móviles

			prohibirá el cambio de la longitud de la contraseña y los requisitos de autenticación	

Tabla 4: Indicadores acceso y privilegio

4.2. Entorno físico[20]

A continuación se describen cada uno de los indicadores elegidos para el ámbito "Entorno físico" así como la medida propuesta para cada uno de ellos. Estos indicadores se definen en la Tabla 5.

20 *Seguridad física* 15/03/2015 <http://www.segu-info.com.ar/fisica/seguridadfisica.htm>

ENTORNO FÍSICO				
Gestión de la continuidad	GC-01	Servicios de centro de datos	Los servicios de centros de datos y las condiciones medioambientales deben ser seguras, monitorizadas, mantenidas y probadas para comprobar su continua funcionalidad en intervalos de tiempo concretos para garantizar la protección de la intercepción no autorizada o daños	Tiempo total interrupción/Tiempo total
	GC-02	Riesgos medioambientales	La protección física contra daños naturales y desastres deben ser anticipados, diseñados y existir contramedidas	Nº de riesgos medioambientales sin medida de contención/Nº total de riesgos medioambientales
	GC-03	Localización del equipamiento	Para reducir los riesgos medioambientales, los peligros y las oportunidades de acceso no autorizado, los equipos deben mantenerse alejados de lugares expuestos a riesgos medioambientales de alta probabilidad y complementados con más equipos situados a una distancia razonable	Nº equipos que cumplen los requisitos/Nº total de equipos
Gestión del centro de datos	GCD-01	Políticas	Las políticas y los procedimientos serán establecidos y el apoyo a los procesos de negocio implementados para mantener un ambiente de trabajo seguro y áreas seguras	Número de áreas seguras/Número total de áreas
	GCD-02	Autorización de área de seguridad	Los puntos de entrada y salida para asegurar áreas seguras, serán limitados y controlados por mecanismos de control de acceso físico que garantice el acceso sólo a personal autorizado	Número de puntos de acceso controlados/Número total de puntos de acceso

	GCD-03	Entrada no segura	Se deberán controlar las entradas sin credenciales que se puedan realizar a los diferentes sistemas	Número de entradas no seguras/Número total de entradas
Gestión de acceso	GA-01	Puntos de control de acceso	Se deben establecer perímetros de seguridad para salvaguardar los datos sensibles y la información de sistemas	Número de puntos de control de acceso seguros/Número total de puntos de control de acceso
	GA-02	Acceso de usuarios	El acceso físico a los activos de información de los usuarios y personal de apoyo será restringido	Número de accesos físicos restringidos/Número total de accesos
	GA-03	Entrada no autorizada	Los puntos de entrada y salida estarán controlados y si es posible aislados de zonas con datos para evitar la corrupción y pérdida de datos	Número de entradas no autorizadas/Número total de entradas

Tabla 5: Indicadores entorno físico

4.3. Integridad de datos[21]

A continuación se describen cada uno de los indicadores elegidos para el ámbito "Integridad de datos" así como la medida propuesta para cada uno de ellos. Estos indicadores se definen en la Tabla 6.

21 *Seguridad de la información y protección de datos* 12/03/2015 <https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/>

INTEGRIDAD DE DATOS				
Seguridad de datos y administración del ciclo de vida de la información	SDACV-01	Integridad de datos	Las funciones de integridad de entrada y salida de datos deben ser implementadas para interfaces de aplicación y bases de datos para prevenir el procesamiento de errores manuales o sistemáticos	Número de funciones con errores/Número total de funciones
	SDACV-02	Clasificación	Los datos y objetos que contengan datos deberán estar clasificados atendiendo al tipo de datos, origen de la jurisdicción, domicilio de la jurisdicción, contexto, restricciones legales, restricciones contractuales, valor, sensibilidad, criticidad hacia la organización, retenciones de terceros y prevención de acceso no autorizado, divulgación o uso indebido	Número de datos clasificados/Número total de datos
	SDACV-03	Política de seguridad	Las políticas y procedimientos se establecerán para el etiquetado, manipulación y la seguridad de los datos y los objetos que contienen datos. Los mecanismos de herencia de etiquetado se implementarán para los objetos que actúan como contenedores agregados de datos	Número de datos etiquetados/Número total de datos
	SDACV-04	Fuga de información	Los mecanismos de seguridad deben ser implementados para prevenir las fugas de información	Número de operaciones con pérdidas de información/Número total de operaciones
	SDACV-05	Propiedad/ Administración	Todos los datos serán administrados, con responsabilidades bien definidas, documentados y comunicados	Número de datos con responsabilidad asignada/Número total de datos
	SDACV-06	E-commerce	Los datos relacionados con el comercio electrónico	Número de datos de

			que utilizan redes públicas deberán estar debidamente clasificados y protegidos de actividades fraudulentas, divulgación no autorizada o modificación para evitar conflicto y compromiso de los datos	e-commerce clasificados/Número total de datos de e-commerce
Cifrado y gestión de claves	CGC-01	Generación de claves	Las políticas y los procedimientos serán establecidas y los procesos de apoyo de negocio y las medidas técnicas serán implementadas para la gestión criptográfica de claves en criptosistemas de servicios. Previa solicitud, el proveedor deberá informar al cliente de los cambios en el sistema de cifrado, especialmente si los datos de cliente son utilizados como una parte del servicio o si el cliente tiene alguna responsabilidad en la implementación de control	Número de criptosistemas con clave/Número total de criptosistemas
	CGC-02	Protección de datos sensibles	Las políticas y procedimientos serán establecidos y el apoyo a los procesos de negocio y medidas técnicas serán implementadas para el uso de protocolos de encriptado para el almacenamiento de datos sensibles y la transmisión de datos según el cumplimiento legal	Número de datos sensibles protegidos/Número total de datos sensibles
	CGC-03	Almacenamiento y acceso	Las claves no se podrán almacenar en la nube. El mantenimiento y uso de claves deben ser tareas separadas	Número de claves almacenadas en la nube/Número total de claves
Seguridad virtual y móvil	SVM-01	Seguridad/Protección de datos	Los canales de comunicación seguros y encriptados deben ser usados cuando se migren servidores físicos, aplicaciones o datos virtualizados, y cuando sea posible se utilizará una red segregada de redes a	Número de migraciones seguras/Número de migraciones totales

			nivel de producción	
	SVM-02	Cifrado	La política de dispositivo móvil requerirá el uso de cifrado para todo el dispositivo o para los datos identificados como sensibles en todos los dispositivos móviles mediante dispositivos tecnológicos	Número de dispositivos móviles cifrados/Número total de dispositivos móviles
	SVM-03	Almacenamiento de datos seguros en la nube	Los datos almacenados en la nube tendrán que estar protegidos y deberá verificarse su seguridad	Número de datos almacenados en la nube de forma segura/Número total de datos

Tabla 6: Indicadores integridad de datos

5. Priorización de indicadores de seguridad[22]

Hasta el momento se han obtenido los indicadores y posibles medidas ordenados y clasificados por tmática y jerarquía a tres ámbitos de la preservación de datos dentro de las tecnologías de la información.

A la hora de aplicar el índice de seguridad a las diferentes alternativas, es necesario saber qué ámbitos o que indicadores de forma individual tienen más importancia o realizan una mayor contribución respecto a los demás para poder establecer una jerarquía entre ellos.

Para obtener el peso (contribución) de cada uno de los indicadores se utiliza un método de decisión multicriterio ya que se ajusta perfectamente al tipo de problema que estamos analizando, de modo que para cada uno de los indicadores expuestos en el punto 3, se puede establecer su nivel de contribución al ámbito y sub-ámbito de seguridad al que pertenece.

5.1. Métodos de decisión multicriterio[23]

A la hora de tomar una decisión para resolver un problema es necesario llevar a cabo un proceso de análisis entre las diferentes opciones existentes para seleccionar la solución que mejor responda ante las necesidades expuestas. En general, a la hora de resolver un problema seguimos los siguientes pasos:

22 *Análisis multicriterio* 25/04/2015 <http://www.ccee.edu.uy/ensenian/catmetad/material/MdA-Scoring-AHP.pdf>
23 *Decisión multicriterio* 25/04/2015 <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-35922007000200004>

Figura 5: Proceso de resolución de problemas

Siguiendo el proceso expuesto en la Figura 5 se puede llegar a la solución de un problema de una manera sencilla. Sin embargo cuando se trata de resolver un problema que cuenta con un número elevado de criterios, la resolución del mismo se complica. Ante este tipo de problemas surgen los métodos de decisión multicriterio.

Los métodos de decisión multicriterio son utilizados para encontrar una solución óptima a un problema teniendo su base sustentada en elementos científicos para asumir una decisión. En todo caso se trata de asumir decisiones basadas en componentes cuantificables que permiten ponderar el peso, y por tanto, elegir la solución que en el mejor de los casos resulte ser la más satisfactoria y en el peor la menos insatisfactoria.

Los métodos de decisión multicriterio son aplicables a aquellos problemas cuyo número de alternativas de decisión es finito. Debe existir una alternativa por cada uno de los factores que se van a considerar y han de evaluarse. Suele utilizarse un método de evaluación sencillo basado en la preferencia entre opciones (A, B, C, etc.) o pequeñas escalas numéricas.

Los principios de los métodos multicriterio provienen de la Teoría de Grafos, la Teoría de Matrices y la Teoría de las Organizaciones y tienen un gran fundamento matemático. El análisis multicriterio puede ser de gran ayuda en la etapa de planificación de un proyecto ya que permite integrar diferentes criterios de acuerdo a varias opiniones diferentes.

A continuación se van a analizar los principales métodos multicriterio utilizados para la resolución de problemas para decidir cual es el que mejor se ajusta al problema tratado en el presente Trabajo de Fin de Grado.

5.1.1. Scoring (ponderación lineal)[24]

El método de scoring o ponderación lineal es uno de los más utilizados cuando se trata de realizar una decisión multicriterio. Con este método se obtiene una puntuación global mediante la suma de las contribuciones de cada uno de los elementos. En caso de que los elementos a evaluar tengan diferentes escalas de medición, es necesario realizar previamente un trabajo de normalización para poder realizar los cálculos del método sin problemas.

Este método cuenta con varias fases:

1. Determinación del objetivo a conseguir
2. Identificación de las alternativas
3. Selección de los criterios a utilizar en la toma de decisiones
4. Asignación de la ponderación
5. Calcular la puntuación para cada una de las alternativas
6. Revisar el efecto de los criterios y ponderaciones en los resultados obtenidos
7. Selección de la alternativa a emplear en función de los resultados obtenidos

24 *Ponderación Lineal* 25/04/2015 <http://www.uv.es/asepuma/XI/07.pdf>

5.1.2. MAUT (utilidad multiatributo)[25]

El método de utilidad multiatributo proporciona una base formal para realizar elecciones entre alternativas cuyas consecuencias están caracterizadas por múltiples atributos. Este método discierne entre la teoría descriptiva y la prescriptiva, definiendo de este modo métodos MAUT descriptivos, que pretenden explicar los intercambios que llevan a cabo los decisores y modelos MAUT prescriptivos que son diseñados para ayudar a los decisores a llevar a cabo sus intercambios para lograr mejores decisiones.

Por otro lado, este modelo distingue también entre decisiones bajo certidumbre y decisiones bajo incertidumbre. En el primer caso los decisores cuentan con información precisa, mientras que en el segundo la información que se conoce es parcial.

Los métodos de utilidad multiatributo, se basan en estimar una función parcial para cada atributo (elementos medibles), teniendo en cuenta las preferencias de la persona encargada de tomar las decisiones, para finalmente generar una única función en forma aditiva o multiplicativa. Al determinarse la utilidad de cada una de las alternativas, se consigue una ordenación del conjunto de las alternativas que intervienen en el proceso.

El método de utilidad multiatributo busca mostrar las preferencias de la persona encargada de tomar las decisiones sobre el conjunto de elementos en base a sus criterios propios.

5.1.3. Relaciones de sobreclasificación[26]

Los métodos basados en relaciones de sobreclasificación tienen su origen en la década de los sesenta y setenta, teniendo un gran número de modificaciones posteriores. Las propuestas realizadas inicialmente se basaban en relaciones binarias denominadas sobreclasificación y en los conceptos de concordancia y discordancia. Estos métodos aparecieron como complemento a la teoría de la utilidad multiatributo.

Se trata de métodos no compensatorios puesto que no se permiten los intercambios entre elementos de la jerarquía. En este método, las preferencias no pueden expresarse mediante una única función numérica.

---

25 *Teoría de la utilidad* 26/04/2015 <http://www.uv.es/asepuma/recta/extraordinarios/Vol_01/03t.pdf>

26 *Métodos multicriterio de ayuda a la decisión* 26/04/2015 <http://www.angelfire.com/ak6/publicaciones/congreso_it_zacatepec.pdf>

A partir de este método y con las modificaciones recibidas, surgieron las distintas versiones de Electre cuyo interés es proponer procedimientos para la solución de diferentes tipos de problemas ocasionados en el tratamiento de la teoría de decisión. Las relaciones de sobreclasificación también son utilizadas en los métodos PROMETE y en los análisis de concordancia en general.

Los principios básicos de las relaciones de sobreclasificación son los siguientes:

- La construcción del modelo de sobreclasificación representa la preferencia total que puede ser formada por uno o más valores o relaciones binarias.
- La explotación del modelo en función del problema a resolver.

A la hora de seleccionar un método de sobreclasificación se tienen en cuenta entre otros, el tipo de resultado que se desea obtener, que tipo de información es posible obtener como datos de entrada y qué propiedades son consideradas importantes en el método.

El método de relaciones de sobreclasificación se utiliza para elegir una solución, que sin ser la óptima, pueda considerarse satisfactoria y por tanto obtener un resultado jerárquico para las alternativas.

5.1.4. Método de decisión multicriterio AHP (análisis jerárquico)

AHP es un método lógico y estructurado que optimiza la toma de decisiones en los casos en los que existen múltiples criterios o atributos. Para ello utiliza la descomposición del problema en una estructura jerárquica de modo que puedan analizarse las contribuciones de los elementos en la jerarquía.

5.2. Elección del método a utilizar: AHP[27]

El método seleccionado para establecer el peso de cada uno de los indicadores de seguridad es el método de decisión multicriterio AHP, también conocido como Proceso de Análisis Jerárquico.

En este modelo es muy importante la figura de los "decisores", que son aquellas personas que realizan su votación sobre los indicadores. El decisor debe establecer la importancia relativa de cada uno de los objetivos (en este caso, de cada indicador de seguridad), para posteriormente establecer una estructura jerarquizada con la que analizar las diferentes alternativas. El resultado final resulta en una clasificación de las alternativas indicando el valor de cada una de ellas y por lo tanto la alternativa que más se ajusta al modelo evaluado.

La principal característica de este método es que el problema a solventar se modeliza mediante una jerarquía en forma de árbol en cuyo vértice superior se encuentra la meta a conseguir, y en la base las posibles alternativas a evaluar. En los niveles intermedios (que pueden formar de nuevo otra jerarquía), se encuentran los criterios en base a los que se toma la decisión.

Otra característica del método AHP, es que en cada nivel de jerarquía se realizan comparaciones entre pares de elementos (en este caso, indicadores de seguridad) de ese propio nivel, teniendo en cuenta la contribución que realiza al elemento de nivel superior al que está ligado. La comparación de elementos dentro de un mismo nivel se basa simplemente en la preferencia del decisor que mostrará mayor interés hacia un elemento u otro.

Una vez evaluada la contribución de cada elemento a los elementos del nivel inmediatamente superior, se procede a calcular la contribución global de cada alternativa al objetivo principal perseguido.

La información obtenida mediante este método puede resultar en ocasiones algo redundante o inconsistente debido al número de evaluaciones/votaciones realizadas. Sin embargo, es esta redundancia la que permite mejorar la exactitud de las valoraciones evitando de este modo un mayor número de errores.

27 *La decisión con apoyo cuantitativo* 25/04/2015 <http://tic.uis.edu.co/ava/pluginfile.php/246973/mod_resource/content/1/M%C3%A9todo%20AHP.pdf>

El método AHP se basa en los siguientes axiomas básicos:

- **Axioma de comparación recíproca:** el decisor debe ser capaz de realizar comparaciones y establecer sus preferencias.
- **Axioma de homogeneidad:** las preferencias son representadas por medio de una escala limitada.
- **Axioma de independencia:** cuando se expresan preferencias, se asume que los criterios son independientes de las propiedades de las alternativas.
- **Axioma de las expectativas:** en la toma de decisiones, se asume que la jerarquía es completa.

El método AHP consta de cinco etapas:

1. **Modelado:** en esta etapa se construye una estructura jerárquica en la que se representan todos los aspectos a tener en cuenta durante la aplicación del modelo.
2. **Valorización:** dentro de esta etapa se establecen las preferencias de cada uno de los decisores involucrados en el proceso de votación. Por cada nivel de la jerarquía, cada decisor debe mostrar su preferencia hacia un elemento u otro tomándolos en pares.
3. **Priorización y síntesis:** esta etapa arroja información global sobre el proceso llevado a cabo. Se trata de tener de forma agregada todas las preferencias establecidas por los diferentes decisores habiendo establecido una escala o porcentaje entre ellas.
4. **Análisis de sensibilidad:** esta última etapa suele realizarse para examinar el grado de sensibilidad del resultado obtenido. Esta etapa puede llevar a modificar alguna de las votaciones realizadas por aparecer inconsistencias entre los datos.

Para la obtención de los resultados del método AHP en el índice de seguridad propuesto en este Trabajo de Fin de Grado se han tenido en cuenta las figuras de dos “decisores”. Estas votaciones han sido realizadas por Víctor García de León González y José María Álvarez Rodríguez, autor y cotutor del presente Trabajo de Fin de Grado respectivamente. La primera votación se corresponde con una visión más técnica de la necesidad de garantizar la seguridad de la información, mientras que la segunda votación está enfocada hacia un nivel de usuario del sistema.

5.3. Ejecución del método AHP

Una vez seleccionado el método AHP para la resolución del problema presentado, para poder aplicar este método a los indicadores expuestos en el punto 3, se ha analizado la estructura jerárquica de los mismos para establecer y analizar el número de niveles. En la Figura 6 se puede observar la estructura definida haciendo referencia a lo expuesto en el apartado “3. Análisis de indicadores de seguridad”.

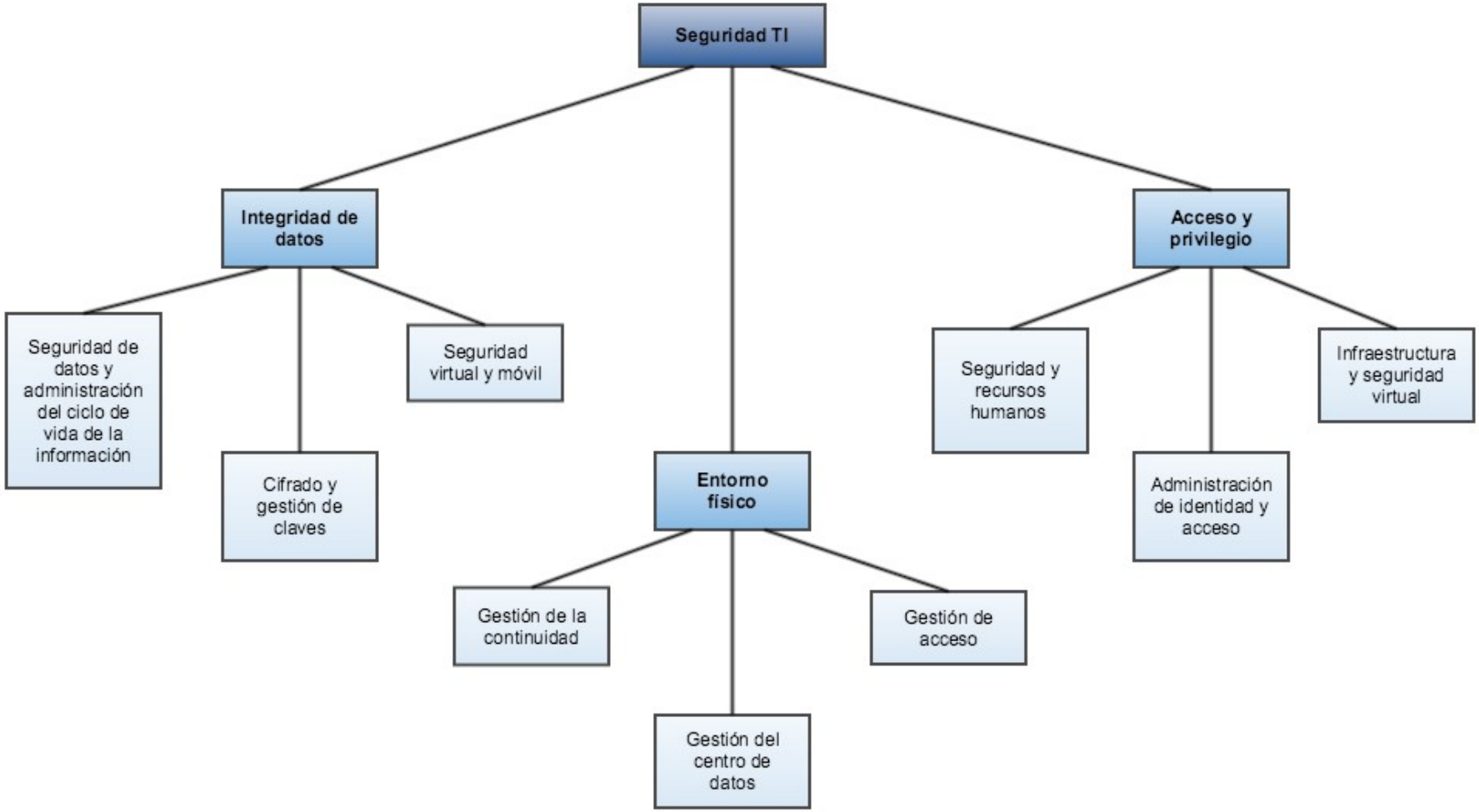


Figura 6: Jerarquía ámbitos del índice de seguridad

Como se puede observar en la Figura 6, existen tres niveles (remarcados en diferente color) en la jerarquía generada para abarcar el índice de seguridad expuesto en el apartado 3 del presente trabajo.

El nivel 1 (azul oscuro) se corresponde con el índice general de los indicadores de seguridad.

El nivel 2 (azul medio) se corresponde con los tres ámbitos de la seguridad seleccionados para este TFG.

El nivel 3 (azul claro) se corresponde con cada uno de los sub-ámbitos (nueve en total) en los que se dividen los ámbitos del segundo nivel para clasificar cada uno de los indicadores definidos en el apartado 3.

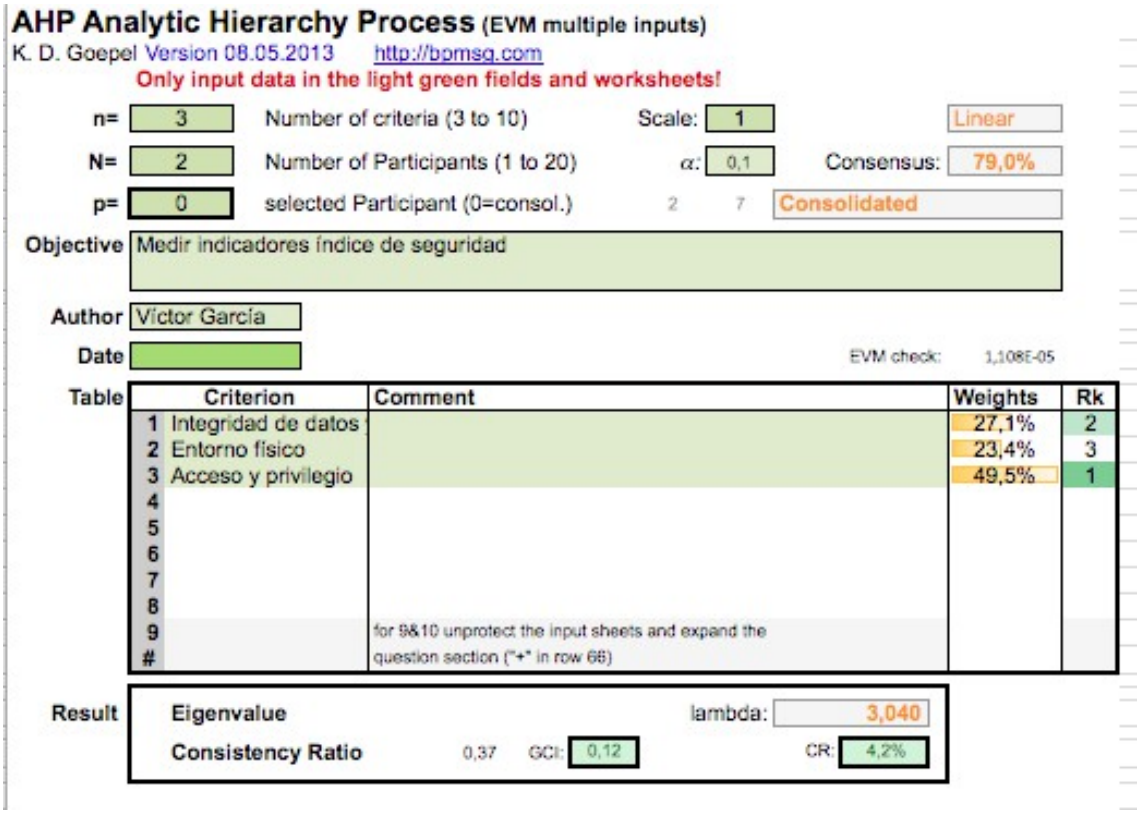
Una vez definida la estructura jerárquica, se procede a aplicar el método AHP mediante hojas Excel ya disponibles para la aplicación.

Tras una búsqueda sobre cómo ejecutar el método AHP, se encontró en http://bpmsg.com un enfoque del método hacia la gestión de rendimiento empresarial (Business Performance Management) que se ajusta perfectamente a las necesidades del presente Trabajo de Fin de Grado. Su autor, K. D. Goepel es un Doctor en Física Alemán de fama y prestigio reconocido, que ha desarrollado una serie de hojas Excel en las que se implementa el método AHP. La elección de éste método se ha debido a la facilidad de uso que presentaba para su aplicación en el TFG, la confianza ofrecida por su autor y el grado de actualización periódica de su sitio web.

A continuación procede a explicar cómo funcionan las hojas Excel seleccionadas para la aplicación del método AHP.

Es necesario crear una hoja de Excel por cada elemento existente en los niveles de la jerarquía y una final en la que se recojan los resultados finales arrojados por el método. En este caso es necesario utilizar catorce hojas de Excel: una para el primer nivel, tres para el segundo nivel, nueve para el tercer nivel y una con los resultados finales de forma agregada.

El formato de las hojas Excel empleadas es el mismo en todos los casos. A continuación se muestra un ejemplo del documento creado para el primer nivel para proceder a su explicación.



AHP Analytic Hierarchy Process (EVM multiple inputs)

K. D. Goepel Version 08.05.2013 http://bpmsg.com

Only input data in the light green fields and worksheets!

n=	3	Number of criteria (3 to 10)	Scale:	1	Linear
N=	2	Number of Participants (1 to 20)	α:	0,1	Consensus: 79,0%
p=	0	selected Participant (0=consol.)	2	7	Consolidated

Objective: Medir indicadores índice de seguridad

Author: Víctor García

Date:

EVM check: 1,108E-05

Table

	Criterion	Comment	Weights	Rk
1	Integridad de datos		27,1%	2
2	Entorno físico		23,4%	3
3	Acceso y privilegio		49,5%	1
4				
5				
6				
7				
8				
9		for 9&10 unprotect the input sheets and expand the		
#		question section ("+" in row 66)		

Result

Eigenvalue lambda: 3,040

Consistency Ratio 0,37 GCI: 0,12 CR: 4,2%

Figura 7: AHP General Nivel 1

En la Figura 7 se puede observar la configuración del método AHP en la hoja de Excel. Esta figura se corresponde con el primer paso a realizar donde es necesario indicar el número de criterios a evaluar (n), en este caso tres ya que el primer nivel se corresponde con los tres ámbitos de la seguridad elegidos para el análisis. También se ha de rellenar el número de participantes (N), en este caso dos, que se corresponden con el autor y cotutor del presente Trabajo de Fin de Grado. Por último, es necesario definir cada uno de los criterios habilitados (n) en la tabla, que se corresponden con los diferentes niveles de la jerarquía.

Una vez realizada la configuración inicial se pueden realizar las diferentes votaciones para cada uno de los criterios establecidos.

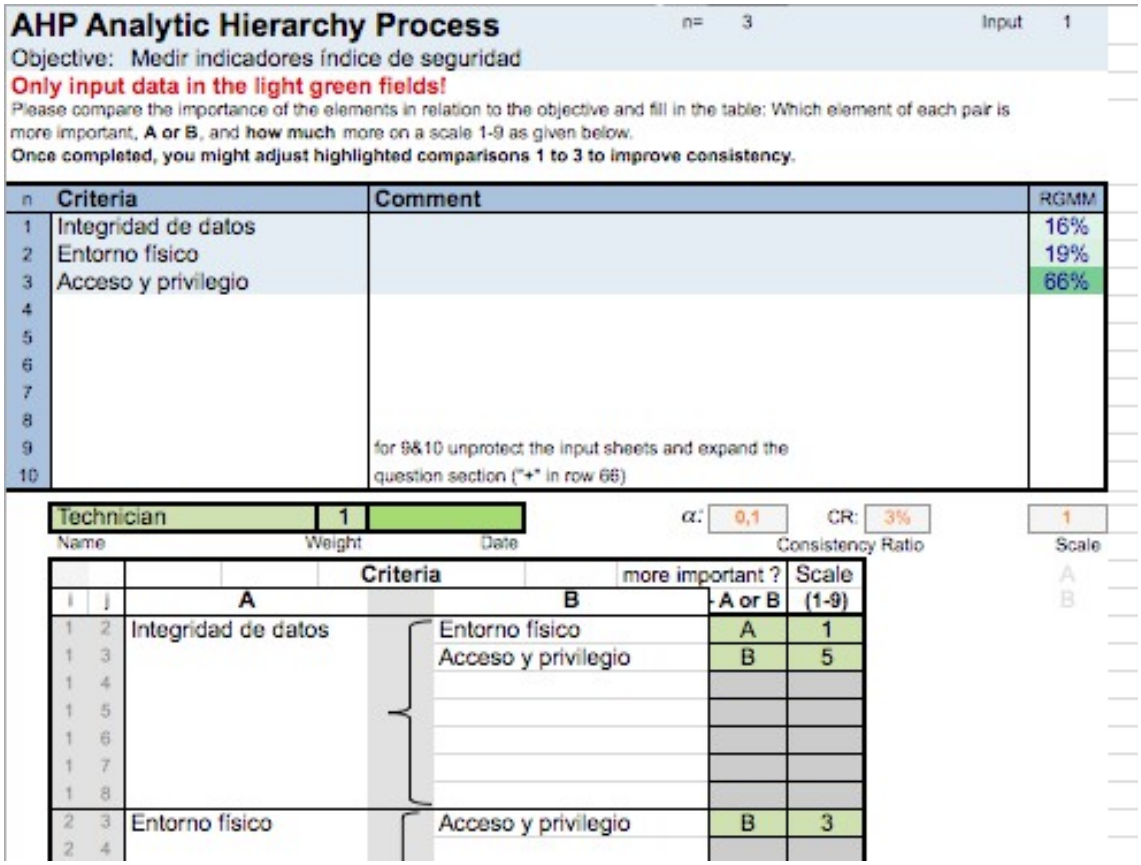


Figura 8: Votación AHP Nivel 1

En la Figura 8 se puede observar una votación realizada para los criterios establecidos en el primer nivel. Sólo es necesario rellenar los cuadros en verde dentro de la tabla, ya que el resto se rellena automáticamente una vez se realizan los pasos descritos anteriormente.

A la hora de realizar las votaciones hay que tener en cuenta la columna **A** y **B** seleccionando pares de dos elementos (uno de la columna A y otro de la B) y decidiendo si tiene más importancia (atendiendo a las preferencias personales) la primera o la segunda columna. Además, se debe establecer una votación numérica en el rango 1-9 según la importancia que se considere que tiene cada indicador.

En documento Excel existe una pestaña de votación por cada decisor involucrado en la ejecución del método.

Una vez que todos los decisores han votado se puede observar los resultados obtenidos para los criterios involucrados en dicho nivel. Estos resultados se calculan y actualizan automáticamente con las votaciones que se realizan.

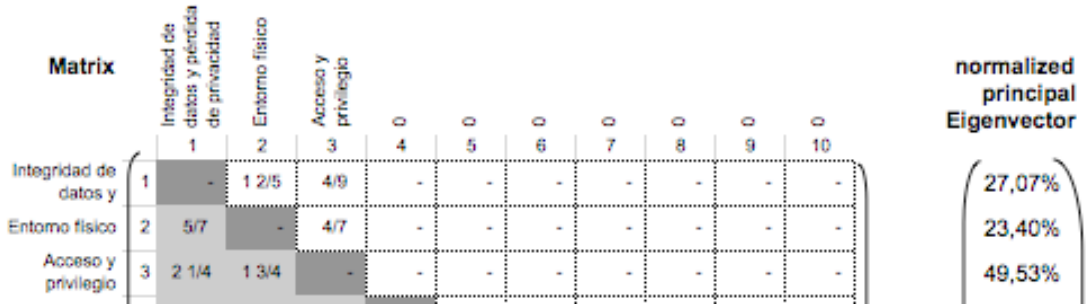


Figura 9: Resultados AHP Nivel 1

En la Figura 9 se pueden observar los resultados obtenidos para los indicadores analizados del primer nivel. Los resultados siempre se obtienen respecto a un total del 100%. Se puede comprobar que el primer ámbito (integridad de datos) aporta un 27,07%, el segundo (entorno físico) un 23,40% y el tercero (acceso y privilegio) un 49,53%.

Una vez se ha explicado un ejemplo de cómo se va a utilizar el método AHP mediante Excel para la realización de este TFG, se seguirán los mismos pasos para cada uno de los documentos Excel generados por cada nivel.

Una vez se hayan realizado todas las votaciones de los diferentes niveles en las hojas Excel, se procederá a juntar los resultados en una única hoja de dicho programa (resultados agregados).

5.4. Resultados obtenidos

Una vez realizadas las votaciones por parte de los dos decisores involucrados de cada una de las hojas Excel y siguiendo los pasos descritos en el apartado anterior, se procede a la obtención de los resultados finales.

Para ello es necesario trasladar los datos individuales de cada una de las hojas Excel a una general (agregado). En esta nueva hoja se van a almacenar cada uno de los pesos obtenidos para cada indicador y se procederá a la normalización de los mismos.

La normalización de los pesos (contribuciones) de cada indicador es necesaria para poder unificar en un solo documento todos los valores. Es decir, en cada hoja Excel referente a un nivel, tenemos los resultados sobre el 100% que representa dicho nivel, por lo tanto se va a proceder a calcular la contribución de cada indicador respecto a un único 100% que se corresponde con la totalidad del índice de seguridad creado. Para realizar esta normalización es necesario, para cada indicador, multiplicar su peso o contribución por la contribución que aporta su padre en la jerarquía. De este modo se obtiene fácilmente los nuevos valores para los indicadores de forma normalizada.

Una vez realizados estos pasos, se obtiene la contribución de cada uno de los indicadores que se han analizado en el índice de seguridad propuesto. A continuación se muestran las secciones de la hoja Excel en las que se encuentran estos resultados.

En la Tabla 7 se pueden observar los resultados obtenidos tras la aplicación del método AHP para cada uno de los indicadores pertenecientes al ámbito de "Acceso y privilegio".

Indicador	Peso Indicador
Acceso y privilegio	**0,494**
Seguridad y recursos humanos	**0,287**
Requisitos de acceso	0,072
Identificación equipamiento	0,031
Administración de dispositivos móviles	0,042
Roles/Responsabilidades	0,095
Espacio de trabajo	0,047
Administración de identidad y acceso	**0,092**
Herramientas de auditoría de acceso	0,009
Ciclo de vida de credenciales/Administración de privilegios	0,012
Políticas y procedimientos	0,019
Segregación de funciones	0,009
Restricciones de acceso a código fuente	0,008
Acceso de terceros	0,006
Fuentes confiables	0,012
Autorización de acceso de usuarios	0,017
Infraestructura y seguridad virtual	**0,115**
Auditoría de acceso/Detección de intrusos	0,029
Seguridad en la red	0,020
Segmentación	0,011
Seguridad VMM	0,016
Seguridad inalámbrica	0,020
Contraseñas	0,019

Tabla 7: Resultados AHP Acceso y privilegio

En la Tabla 8 se pueden observar los resultados obtenidos tras la aplicación del método AHP para los indicadores pertenecientes al ámbito de "Entorno físico".

Indicador	Peso Indicador
Entorno físico	**0,233**
Gestión de la continuidad	**0,083**
Servicios de centro de datos	0,034
Riesgos medioambientales	0,021
Localización equipamiento	0,028
Gestión del centro de datos	**0,043**
Políticas	0,016
Autorización de área de seguridad	0,019
Entrada no segura	0,008
Gestión de acceso	**0,107**
Puntos de control de acceso	0,041
Acceso de usuarios	0,015
Entrada no autorizada	0,051

Tabla 8: Resultados AHP Entorno físico

Los resultados obtenidos para los indicadores pertenecientes al ámbito "Integridad de datos" pueden observarse en la Tabla 9.

Indicador	Peso Indicador
Integridad de datos	**0,270**
Seguridad de datos y administración del ciclo de vida de la información	**0,162**
Integridad de datos	0,022
Clasificación	0,008
Política de seguridad	0,036
Fuga de información	0,054
Propiedad/Administración	0,017
E-Commerce	0,025
Cifrado y gestión de claves	**0,042**
Generación de claves	0,005
Protección de datos sensibles	0,026
Almacenamiento y acceso	0,011
Seguridad virtual y móvil	**0,066**
Seguridad/Protección de datos	0,030
Cifrado	0,012
Almacenamiento de datos seguros en la nube	0,024

Tabla 9: Resultados AHP Integridad de datos

En las Tablas 7, 8 y 9 se puede observar el nivel de contribución para cada clasificación realizada dentro de los tres ámbitos de seguridad elegidos (acceso y privilegio, entorno físico e integridad de datos) para el índice de seguridad. Además, se puede comprobar cuál es el nivel de contribución de cada uno de los indicadores en la clasificación a la que pertenecen.

5.5. Análisis de los resultados

A continuación se incluye una tabla resumen (Tabla 10) con los resultados obtenidos tras la aplicación del método AHP para la clasificación realizada de los ámbitos de seguridad escogidos. Los pesos por indicador pueden encontrarse en las Tablas 7, 8 y 9.

Indicador	Peso
Acceso y privilegio	**0,494**
Seguridad y recursos humanos	0,287
Administración de identidad y acceso	0,092
Infraestructira y seguridad virtual	0,115
Entorno físico	**0,233**
Gestión de la continuidad	0,083
Gestión del centro de datos	0,043
Gestión de acceso	0,107
Integridad de datos	**0,270**
Seguridad de datos y administración del ciclo de vida de la información	0,162
Cifrado y gestión de claves	0,042
Seguridad virtual y móvil	0,066

Tabla 10: Resumen resultados AHP

En la Tabla 10 se puede observar la contribución realizada al índice de seguridad por cada uno de los ámbitos y sub-ámbitos seleccionados.

Partiendo de la Figura 6 en la que se definió la estructura jerárquica del índice de seguridad, se ha realizado un nuevo diagrama de árbol en el que se puede observar la distribución de los pesos (contribuciones) que tienen los diferentes ámbitos y sub-ámbitos. Gracias a este diagrama se puede comprobar de forma sencilla como se distribuyen los pesos en los diferentes niveles. La Figura 10 se corresponde con éste diagrama.

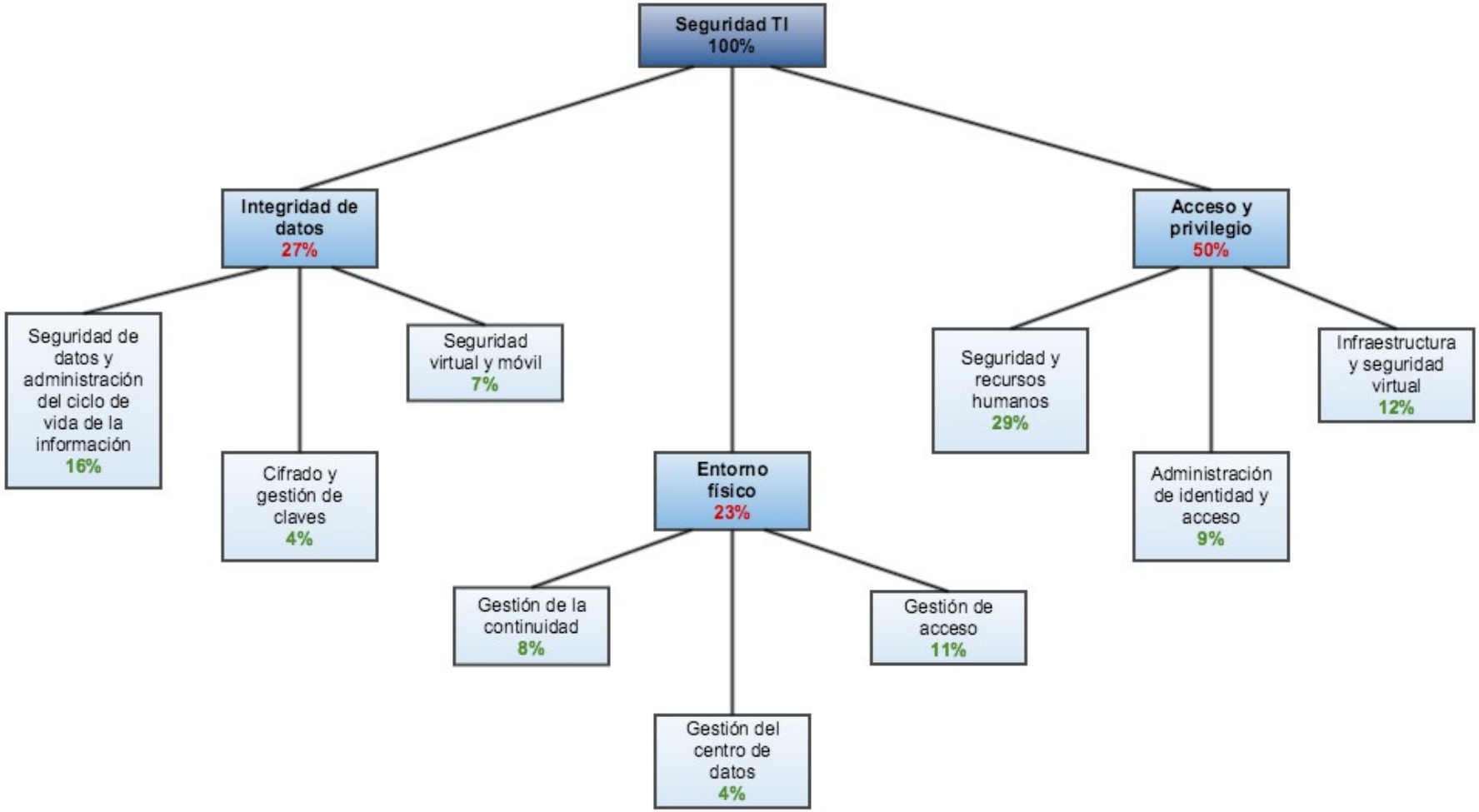


Figura 10: Jerarquía ámbitos del índice de seguridad con contribuciones

Para poder realizar un mejor análisis se van a representar los resultados obtenidos en la Tabla 10 de forma gráfica para comprobar de forma visual las contribuciones realizadas por los diferentes ámbitos y sub-ámbitos.

Atendiendo sólo a los tres ámbitos de seguridad seleccionados para la elaboración del índice de seguridad se obtiene el siguiente gráfico:

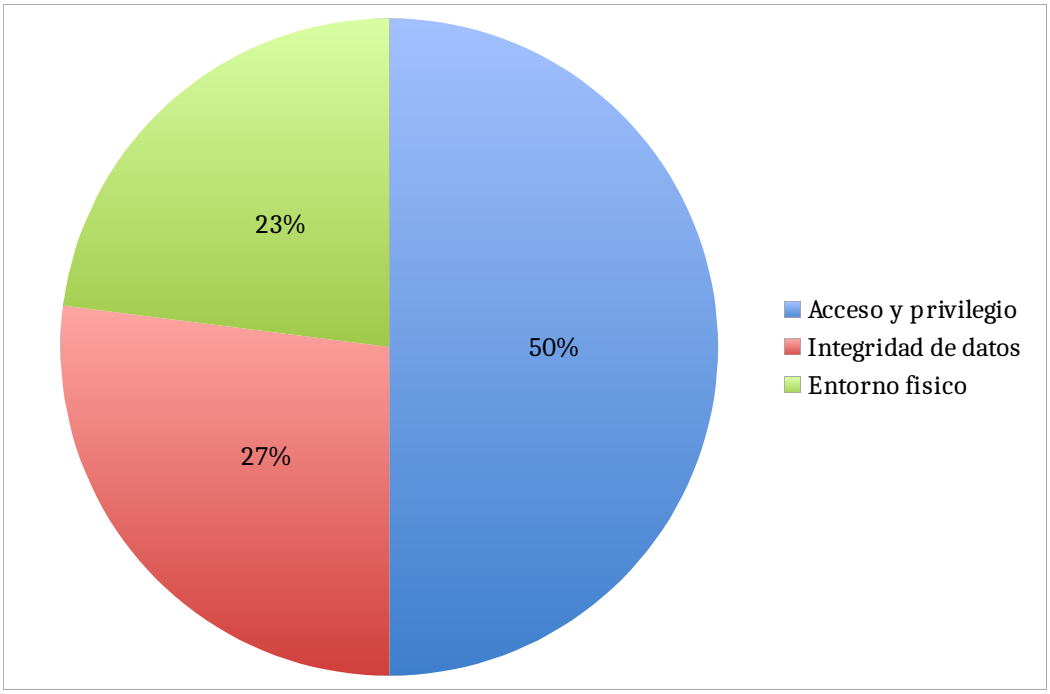


Figura 11: Resultados AHP ámbitos generales

En la Figura 11 se puede observar de forma muy simple que el ámbito de acceso y privilegio es el más valorado tras haber aplicado el método AHP puesto que ocupa el 50% del porcentaje total. En segundo lugar se encuentra el ámbito de integridad de datos con un 27% y por último, entorno físico ocupando el 23% restante.

Los datos obtenidos están directamente relacionados con los decisores involucrados en el método AHP puesto que se tiene en cuenta sus preferencias durante el proceso de votación de los indicadores de seguridad establecidos para el índice de seguridad. Atendiendo a esto, los resultados podrían variar en gran medida si se tuviesen en cuenta los puntos de vista de otros decisores. Si se contase con un mayor número de votaciones, existirá una mayor disparidad de datos en cuanto a las preferencias y por lo tanto existiría un mayor equilibrio en los resultados. Sin embargo, como se indicó anteriormente, para el presente Trabajo de Fin de Grado se ha creido conveniente tener en cuenta solo dos puntos de vista para analizar el comportamiento de los datos y resultados atendiendo a un perfil técnico y otro a nivel usuario.

Por otro lado, se analizan de forma gráfica (Figura 12) la aportación realizada por cada uno de los sub-ambitos en los que se ha subdividido los tres ámbitos principales. La aportación de cada sub-ámbito se calcula mediante la suma de las diferentes contribuciones de sus indicadores.

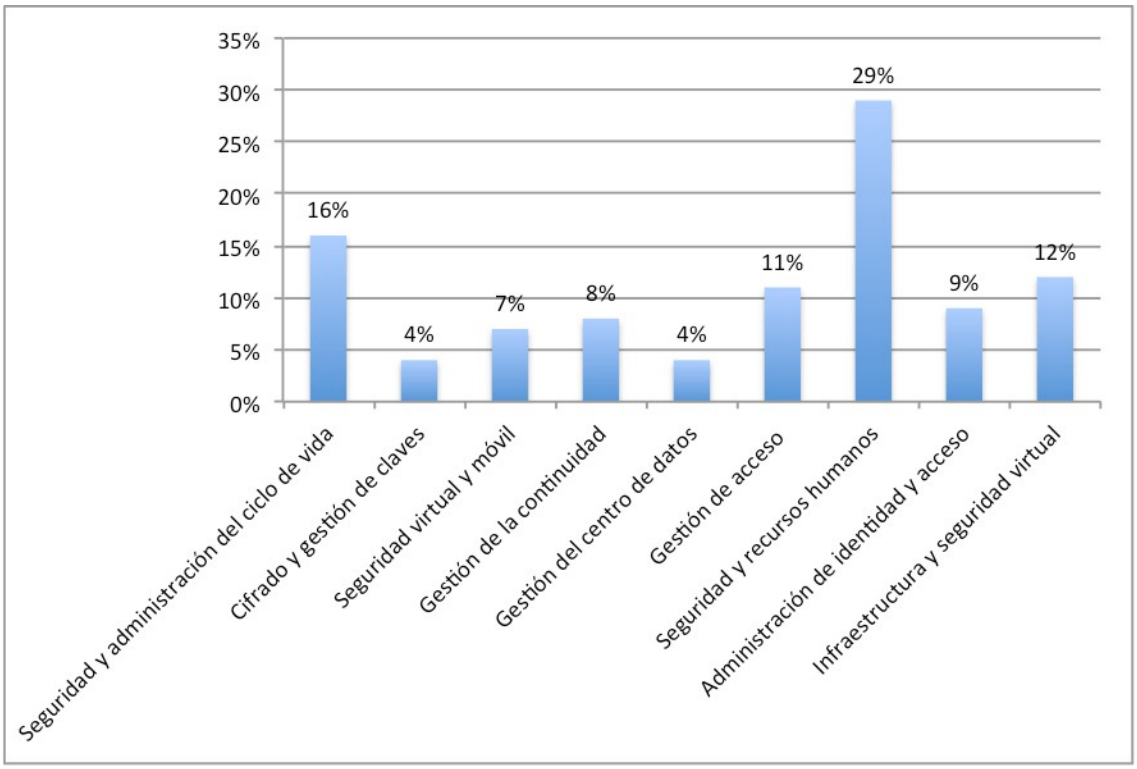


Figura 12: Resultados AHP sub-ámbitos

Como se puede observar en la Figura 12 el sub-ámbito de seguridad y recursos humanos (perteneciente al ámbito de acceso y privilegio) es el que más contribución realiza al índice de seguridad puesto que aporta un 29% del total. Los siguientes más importantes son seguridad y administración del ciclo de vida con un 16%, infraestructura y seguridad virtual aportando un 12% o gestión de acceso con un 11%. El resto de sub-ámbitos se dividen el resto del porcentaje de una forma parcialmente equitativa.

De nuevo estos resultados están condicionados por las preferencias aportadas por cada uno de los decisores que han realizado las votaciones. Un mayor tamaño de muestra en las votaciones aportaría resultados más equitativos.

Una vez analizados los resultados de forma general, atendiendo sólo a los ámbitos y sub-ámbitos del índice de seguridad, resulta interesante conocer a nivel individual de indicador la aportación que realizan al sub-ámbito al que pertenecen cada uno de éstos. Para esto se incluye un diagrama de árbol por cada sub-ámbito de modo que se represente gráficamente la contribución realizada por cada indicador.

Acceso y privilegio:

La contribución realizada por cada indicador dentro del sub-ámbito "Seguridad y recursos humanos" se define de la siguiente forma:

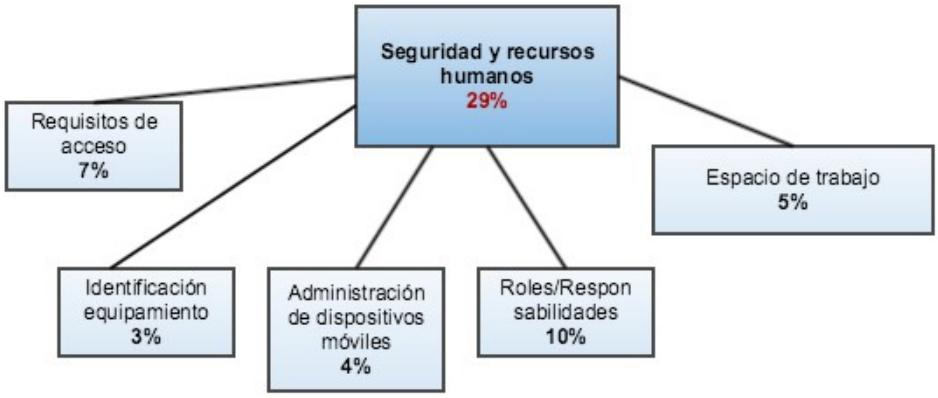


Figura 13: Contribuciones "Seguridad y recursos humanos"

En la Figura 13 se puede observar que el sub-ámbito "seguridad y recursos humanos" es uno de los más importante puesto que contribuye un 29% al índice de seguridad. Los indicadores que mas contribuyen a este porcentaje son "roles/responsabilidades" y "requisitos de acceso".

La contribución realizada por cada indicador dentro del sub-ámbito "Administración de identidad y acceso" queda definida de la siguiente forma:

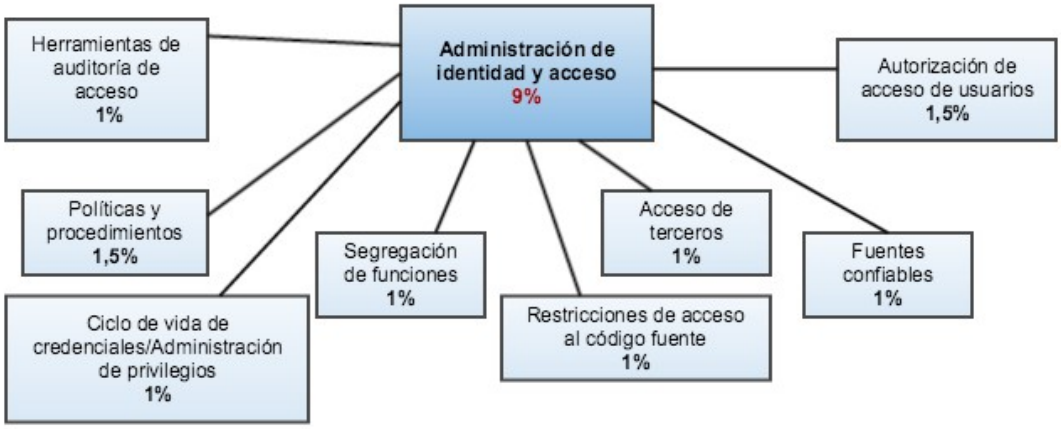


Figura 14: Contribuciones "Administración de identidad y acceso"

En la Figura 14 se puede comprobar que los indicadores con mayor importancia dentro de este sub-ámbito son "políticas y procedimientos" y "autorización de acceso de usuarios".

La contribución realizada por cada indicador dentro del sub-ámbito "Infraestructura y seguridad virtual" queda definida de la siguiente forma:

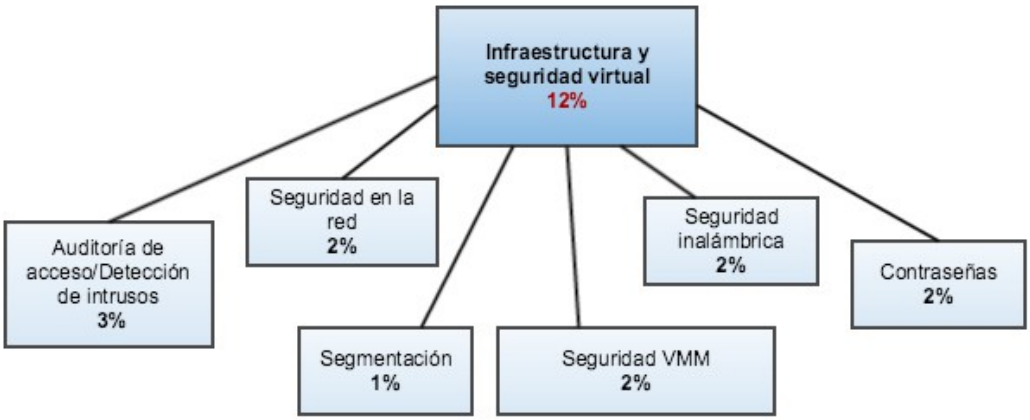


Figura 15: Contribuciones "Infraestructura y seguridad virtual"

En la Figura 15 se observa que dentro del sub-ámbito "infraestructura y seguridad virtual" la mayor contribución viene realizada por el indicador "auditoria de acceso/detección de intrusos".

Entorno físico:

La contribución realizada por cada indicador dentro del sub-ámbito "Gestión de la continuidad" se define de la siguiente forma:

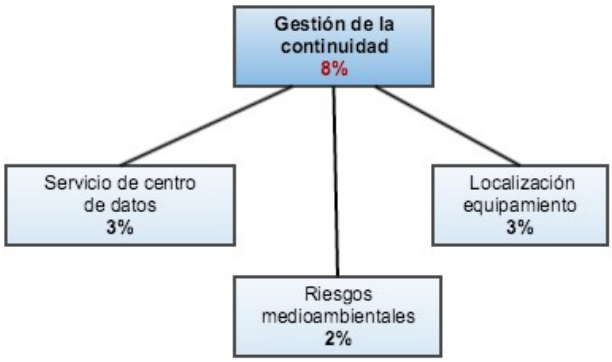


Figura 16: Contribuciones "Gestión de la continuidad"

En la Figura 16 se puede observar que dentro del sub-ámbito "gestión de la continuidad", los indicadores que mayor contribución realizan (lo hacen de forma equitativa) son "servicio de centro de datos" y "localización del equipamiento".

La contribución realizada por cada indicador dentro del sub-ámbito "Gestión del centro de datos" se define de la siguiente forma:

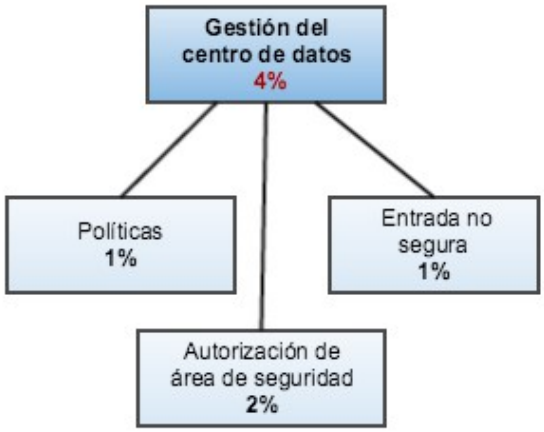


Figura 17: Contribuciones "Gestión del centro de datos"

En la Figura 17 se puede comprobar que tanto el indicador de "políticas" como el de "autorización de área de seguridad" son los que mayor contribución realizan al sub-ámbito de seguridad al que pertenecen.

La contribución realizada por cada indicador dentro del sub-ámbito "Gestión de acceso" queda definida de la siguiente forma:

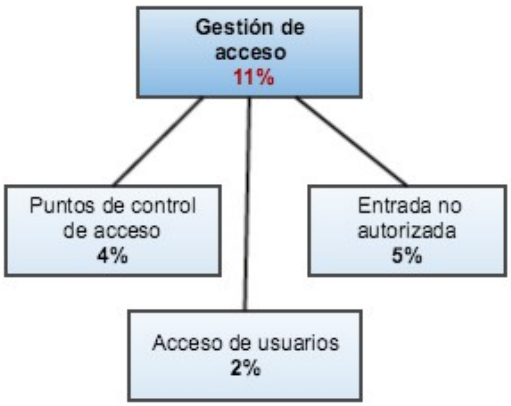


Figura 18: Contribuciones "Gestión de acceso"

En la Figura 18 se puede comprobar que el indicador referente a la entrada no autorizada es el que mayor contribución realiza al sub-ámbito "gestión de acceso".

Integridad de datos:

La contribución realizada por cada indicador dentro del sub-ámbito "Seguridad de datos y administración del ciclo de vida de la información" se define de la siguiente forma:

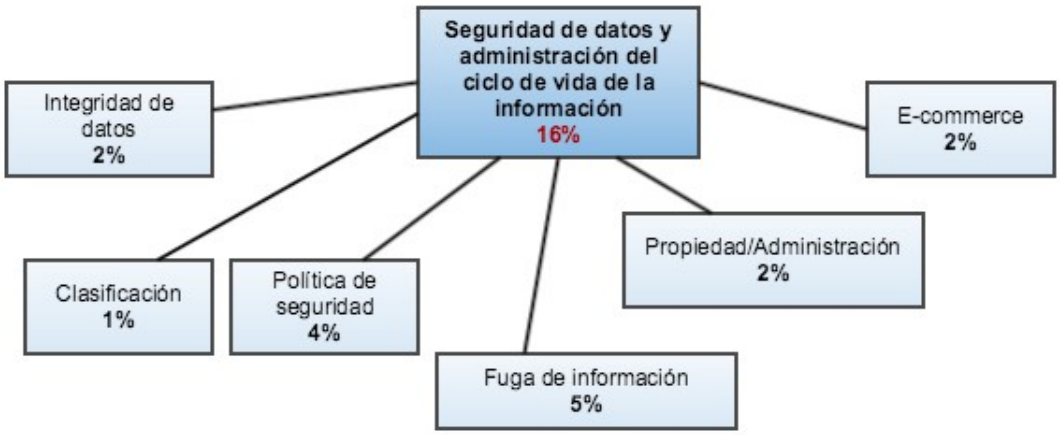


Figura 19: Contribuciones "Seguridad de datos y administración del ciclo de vida de la información"

A partir de la Figura 19 se puede comprobar como los indicadores "fuga de información" y "política de seguridad" son los que mayor contribución realizan a su objetivo de seguridad (sub-ámbito al que pertenecen).

La contribución realizada por cada indicador dentro del sub-ámbito "Cifrado y gestión de claves" queda definida de la siguiente forma:

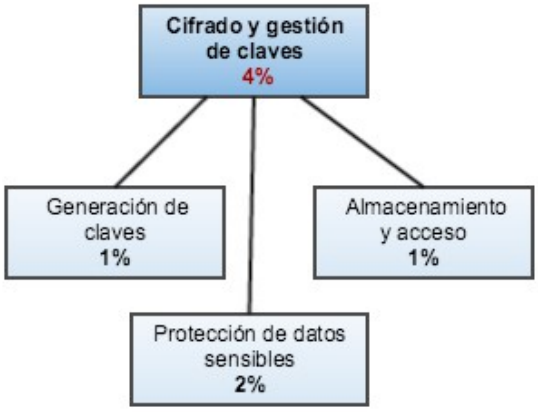


Figura 20: Contribuciones "Cifrado y gestión de claves"

A partir de la Figura 20 se puede comprobar como el indicador "protección de datos sensibles" es el que mayor contribución realiza al sub-ámbito "cifrado y gestión de claves".

La contribución realizada por cada indicador dentro del sub-ámbito "Seguridad virtual y móvil" se define de la siguiente forma:

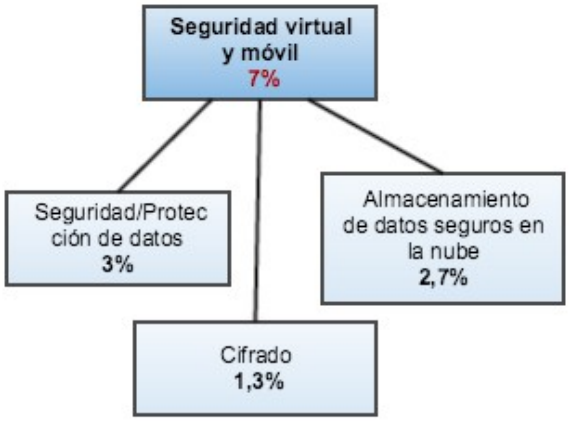


Figura 21: Contribuciones "Seguridad virtual y móvil"

En la Figura 21 se puede observar que dentro del sub-ámbito "seguridad virtual y móvil" el indicador que mayor aportación realiza es el que concierne la seguridad y la protección de datos.

5.6. Interpretación de los resultados

A continuación se va a realizar una interpretación de los resultados y datos obtenidos tras la aplicación del método AHP.

5.6.1. Ámbitos generales del índice de seguridad

Atendiendo exclusivamente a los tres ámbitos de seguridad seleccionados (Figura 11) se puede concluir que el ámbito con mayor importancia es "Acceso y privilegio" puesto que aporta un 50% del total.

Analizando este dato se puede establecer que el resultado obtenido es razonable puesto que un acceso controlado a los datos e información garantiza en gran medida la integridad de los datos. Las consecuencias en una organización de que una persona no autorizada acceda a datos sensibles podrían ser nefastas para la propia organización y para la persona de quien trate la información. Existen diversos métodos muy complejos que se instauran en las empresas y organizaciones para garantizar el acceso y privilegios a los datos tales como "Bell-LaPadula", "BIBA" o la "Muralla China". Los dos primeros métodos están centrados en el acceso a los objetos (datos) por parte de los sujetos (usuarios) otorgándole permisos de lectura y/o escritura según sus permisos. En el caso del método "Muralla China" se controla que usuarios que trabajan en empresas distintas, pero pertenecientes a un mismo grupo de interés, no puedan acceder a información confidencial los unos de los otros.

Dentro de los tres ámbitos de seguridad, el segundo en realizar mayor contribución es "Integridad de datos" que aporta un 27%. Este resultado puede parecer algo inconsistente puesto que si lo que se persigue mediante el índice de seguridad es garantizar los datos e información, cabría esperar que éste ámbito estuviese en primer lugar. Sin embargo, las votaciones realizadas se hacen desde un punto de vista personal (uno enfocado hacia un ámbito técnico y otro de usuario), de modo que teniendo en cuenta que los tres ámbitos han sido seleccionados considerando su importancia para la consecución de la integridad de los datos, se le ha dado más importancia al analizado anteriormente. Dentro de este sub-ámbito se tratan los temas de contraseñas, cifrados, seguridad móvil, etc., y puede que hayan obtenido una menor puntuación al aplicar el método AHP ya que se puede dar por hecho su existencia para garantizar la seguridad de los datos y por tanto restarle importancia en las votaciones, ya que hoy en día no se concebiría ningún sistema de este tipo sin contraseñas, etc.

Por último, el "Entorno físico" aporta un 23% al índice de seguridad. Todo aquello que tenga que ver con el entorno físico es un tema con el que no se está muy familiarizado puesto que en caso de un perfil de usuario no se tienen en cuenta asuntos como los riesgos medioambientales, diferentes localizaciones, etc. En el caso de un perfil técnico, aunque se tienen en cuenta ciertos factores pertenecientes al entorno físico, no se le da la importancia suficiente. Estos motivos hacen que este ámbito sea el que menos contribuye al índice de seguridad.

5.6.2. Sub-ámbitos del índice de seguridad

Teniendo en cuenta los sub-ámbitos establecidos para el índice de seguridad y los resultados obtenidos se puede concluir que el sub-ámbito "Seguridad y recursos humanos" es el más importante en el índice de seguridad. Es necesario entender que el apartado recursos humanos de este sub-ámbito hace referencia a todos los usuarios de los sistemas, analizando el rol que tienen, permisos, operaciones permitidas, requisitos de acceso, etc. Esto guarda consistencia con la información obtenida en el apartado anterior puesto que se daba mayor importancia debido a su contribución al ámbito "Acceso y privilegio" que implica directamente a los usuarios como trata este sub-ámbito.

De nuevo es necesario recordar que los resultados muestran las preferencia de las votaciones realizadas, por lo que otras votaciones podrían variar los mismos.

Atendiendo a la Figura 12, el siguiente sub-ámbito con mayor contribución es "Seguridad y administración del ciclo de vida" aportando un 16%. La contribución de este sub-ámbito es casi la mitad a la anterior, por lo que es un decremento considerable a análsis. Dentro de este sub-ámbito se engloban todos los contenidos referentes a políticas de seguridad, fugas de información, clasificación, etc., a las que un decisor con perfil de usuario no le da demasiado valor debido a su desconocimiento, al contrario que un perfil técnico que ofrecerá una mejor votación. Esta discrepancia es la que marca que el resultado siga siendo importante pero haya bajado en gran medida.

Por último dentro de los sub-ámbitos destaca “Infraestructura y seguridad virtual” con una aportación del 12% que atañe a temas como auditorías de acceso, seguridad en la red, seguridad inalámbrica, etc. De nuevo ocurre lo mismo que en el caso anterior, el perfil técnico valorará los indicadores de este sub-ámbito de forma más elevada que el perfil de usuario y por eso el resultado obtenido.

El resto de sub-ámbitos tienen unos valores muy parecidos. Pueden consultarse en la Figura 12.

5.6.3. Indicadores del índice de seguridad

Una vez analizados los resultados obtenidos de forma general y a nivel de sub-ámbitos se procede a examinar los resultados obtenidos de forma individual para cada indicador. Para ello se analizan las Tablas 7, 8 y 9 en las que se pueden observar los datos de forma individual.

Tras analizar estas tablas se puede comprobar que el indicador “Roles/Responsabilidades” es el más importante puesto que aporta un 10% al índice de seguridad. Este resultado es consistente con lo obtenido anteriormente puesto que se da mayor importancia a los usuarios que tratan con la información y a los permisos o habilitaciones que tienen sobre ella.

En segundo lugar, el indicador “Requisitos de acceso” aporta un 7% al índice siguiendo en la misma línea que el anterior (ambos pertenecen al mismo sub-ámbito). De nuevo esto hace que este sub-ámbito haya sido en términos generales el mejor valorado (el que más contribución realiza).

Por último cabe destacar los indicadores “Fuga de información”, “Entrada no autorizada” y “Espacio de trabajo” que realizan una contribución del 5% respectivamente al índice de seguridad. Estos indicadores pertenecen a distintos sub-ámbitos del índice pero guardan cierta concordancia con los resultados obtenidos en los dos apartados anteriores puesto que se trata de temas que inciden directamente sobre los usuarios que tratan con la información.

El resto de indicadores cuentan con unos valores de contribución muy parecidos. Estos valores pueden comprobarse en las Tablas 7, 8 y 9.

6. Caso de estudio[28,29]

Una vez obtenido el índice de seguridad con los pesos para cada indicador, se procede a su aplicación práctica para la elección de la alternativa que mejor satisfaga los criterios expuestos en él.

El presente Trabajo de Fin de Grado está enfocado hacia la medición de la seguridad para garantizar la integridad de datos a partir de los ámbitos elegidos. Siguiendo esta línea se ha decidido realizar una comparativa entre diferentes sistemas de almacenamiento que ofrecen servicios en la nube. La elección ha sido ésta puesto que dichos sistemas de almacenamiento son muy utilizados hoy en día por un gran número de usuarios para la compartición de diferentes tipos de archivos, en muchos casos de carácter sensible y resulta interesante conocer qué alternativa se adecua mejor al índice desarrollado.

Los sistemas de almacenamiento seleccionados para evaluación mediante el índice de seguridad propuesto son Google Drive, Dropbox y MEGA. La elección ha sido esta ya que personalmente, a lo largo de la carrera, he trabajado con los tres sistemas y según mis necesidades en cada momento he elegido uno u otro. Por este motivo me ha parecido interesante realizar la comparativa entre ellos.

Antes de aplicar el índice sobre los sistemas seleccionados, se va a analizar cada uno de ellos para conocer sus principales características.

6.1. Google Drive[30]

Google Drive es un servicio de almacenamiento y alojamiento de archivos ofrecido por la empresa Google desde Abril de 2012. Este sistema ha ido cambiando los planes de almacenamiento a lo largo del tiempo y actualmente ofrece 15 GB de almacenamiento gratuito a cada usuario, ampliable hasta 30 TB previo pago de una cuota mensual.

Uno de los cambios más notables realizados por Google Drive últimamente ha sido su actualización a Google Docs, que en esencia sigue siendo el mismo sistema de almacenamiento, pero incluye un procesador de texto y hoja de cálculo de forma online. De este modo el usuario puede modificar sus archivos (los que sean de este tipo) directamente desde la versión web gracias a este servicio.

---

28 *Servicios de almacenamiento en la nube* 15/05/2015 <http://computerhoy.com/listas/software/mejores-servicios-gratuitos-almacenamiento-nube-8518>

29 *Almacenamiento en la nube* 15/05/2015 <http://www.elmundo.es/elmundo/2012/04/25/navegante/1335354932.html>

30 *Información Google Drive* 15/05/2015 <https://support.google.com/drive/answer/6558?hl=es>

En cuanto a las versiones ofrecidas, cuenta con versión web (optimizada para el navegador de la empresa Google Chrome), aplicación escritorio para los principales sistemas operativos y aplicaciones para los principales sistemas operativos de dispositivos móviles. El hecho de ser un sistema multiplataforma, hace que un alto porcentaje de usuarios lo utilicen.

A modo de resumen, las principales características de Google Drive son las siguientes:

- Ofrece una cuota de almacenamiento gratuito
- Posibilidad de aumentar el espacio de almacenamiento previo pago de la tarifa pertinente
- Aplicación para ordenador en varios sistemas operativos
- Aplicación para dispositivos móviles de diferentes sistemas operativos
- Posibilidad de trabajo multiusuario en un mismo instante de tiempo
- Integrado con otras aplicaciones de Google

En cuanto a la seguridad ofrecida por Google Drive, se trata de un sistema de almacenamiento seguro puesto que cada usuario debe proporcionar unas credenciales para poder acceder a su cuenta. Estas credenciales vendrán dadas por el e-mail de registro y la contraseña seleccionada, que se almacena de forma cifrada.

El principal problema de seguridad existente en esta plataforma, y en general en todas las de este tipo, viene dado por la capacidad de compartir archivos o carpetas con otros usuarios ya que surgen los conflictos devenidos de los derechos sobre el material almacenado.

Ante este problema existe la posibilidad de seleccionar quien es el propietario de una carpeta y si éste concede o no permisos a otros usuarios para invitar a otros nuevos a dicha carpeta. Un pequeño fallo en la elección de estas características o el desconocimiento de las condiciones por defecto del sistema, podría dejar los archivos accesibles a terceros no deseados.

Una de las grandes críticas a este sistema viene dada por una de las clausulas de privacidad en la que se establece que el usuario concede a Google una licencia para usar, almacenar, alojar (…) y distribuir el contenido almacenado en su cuenta, si bien puntualiza que sólo utilizará los derechos que le confiere esta concesión con el fin de proporcionar, promocionar o mejorar los servicios.

6.2. Dropbox[31,32,33]

Dropbox es un servicio de almacenamiento y alojamiento de archivos multiplataforma en la nube ofrecido por la compañía Dropbox. Esta plataforma vio la luz en Junio de 2007 cuando dos alumnos del MIT decidieron buscar una solución al problema de compartición y sincronización de archivos.

Este servicio ofrece la posibilidad de almacenar y compartir archivos y carpetas con otros usuarios de forma muy sencilla. Pone a disposición del usuario aplicaciones escritorio de los principales sistemas operativos utilizados en la actualidad. Del mismo modo, ofrece aplicaciones para diferentes sistemas operativos de dispositivos móviles.

En cuanto al almacenamiento, Dropbox ofrece dos tipos de registro: particular o empresa. En caso de registro particular, la cuota de partida inicial y gratuita es de 2 GB, ampliable hasta 1 TB previo pago de las cuotas establecidas. Una gran ventaja de Dropbox, y que hace que sea ampliamente utilizado en ciertos sectores de usuarios, es la posibilidad de aumentar el espacio gratuito mediante diferentes promociones entre las que destacan invitar a otros amigos a utilizar Dropbox, ser estudiante, etc. En cuanto a la versión de Dropbox para empresas, es una versión de pago cuyas cuotas difieren según el número de usuarios que se registren para esa empresa y la capacidad deseada, comenzando en 1000 GB y ampliable según necesidades.

En temas de seguridad, al tratarse de un servicio de almacenamiento en la nube y compartición de datos con otros usuarios, de nuevo surge el problema de los derechos y propiedad sobre los archivos alojados, además de quien puede acceder a que cosas.

Como solución al segundo problema, en la versión básica de Dropbox existe la posibilidad de seleccionar quien es el propietario de cada carpeta, elegir quien puede ver los archivos, si todos los integrantes de una carpeta pueden invitar a otros nuevos o si sólo puede hacerlo el propietario, etc.

Por otro lado, en la versión para empresas de Dropbox, los niveles de seguridad aumentan de forma notable. Entre las medidas ofrecidas destacan que los archivos se almacenan de forma segura mediante cifrado AES de 256 bits y las transferencias siempre son realizadas mediante el protocolo SSL. Otros de los servicios de seguridad que ofrece esta versión pueden observarse en la Figura 22.

31 *Dropbox help* 20/05/2015 <https://www.dropbox.com/help>
32 *Dropbox empresas* 20/05/2015 <http://www.xatakaon.com/almacenamiento-en-la-nube/dropbox-lanza-su-version-para-empresas-con-interesantes-novedades>
33 *Cuidado con Dropbox* 20/05/2015 <http://www.genbeta.com/herramientas/cuidado-con-dropbox-podrian-tener-posibilidad-de-acceder-a-tus-archivos>

Figura 22: Características Dropbox[34]

Atendiendo a la Figura 22, cabe destacar las opciones de recuperación de archivos, auditorías de uso compartido y actividad del usuario y borrado remoto y transferencia de cuentas como buenas prácticas para mejorar la seguridad del sistema.

Una de las críticas más recibida hacia este sistema es, pese al trabajo de cifrado de datos en el sistema, la existencia de la posibilidad por parte de Dropbox de acceder a los archivos descifrados mediante técnicas para tal fin (atendiendo a temas legales, sería necesaria una orden judicial para proceder a tal situación). Sin embargo, esta práctica usual tendría como único fin beneficiar al propio usuario, aunque la empresa también lo hace, puesto que con dicho método se ahorra ancho de banda.

34 *Dropbox pricing* 20/05/2015 <https://www.dropbox.com/business/pricing>

6.3. MEGA[35,36]

Mega se trata de un sitio web para el almacenamiento y compartición a nivel público de archivos, principalmente grandes volúmenes de datos disponible desde Enero de 2013. Este servicio es el sucesor de Megaupload cerrado por cuestiones legales.

Este servicio se clasificaría mejor como una plataforma de compartición de grandes volúmenes de datos e intercambio de datos a nivel mundial. Dentro de esta plataforma/servicio existen cuatro tipos de suscripciones: una gratuita que ofrece al usuario un almacenamiento gratuito de hasta 50 GB y tres de pago que incrementan gradualmente su capacidad de almacenamiento hasta los 4 TB.

El tipo de compartición realizado en esta plataforma es diferente a las dos alternativas anteriores puesto que una vez almacenado un archivo, se genera una URL que es la que se comparte y da acceso al recurso en concreto.

Este sistema, a diferencia de los anteriores, no ofrece aplicación escritorio para ningún sistema operativo. Sin embargo, su versión web proporciona al usuario un tipo de extensión instalable en Google Chrome o Mozilla Firefox que facilita su uso. En cuanto a dispositivos móviles, ofrece aplicaciones para los principales sistemas operativos utilizados hoy en día.

En cuanto a la seguridad de los datos que ofrece comienza en el momento en que se sube un archivo puesto que se cifra mediante RSA de 2048 bits. Todos los archivos almacenados en MEGA están cifrados y del mismo modo las transferencias tanto de subida como de bajada al sistema.

La mayor critica que recibe este sistema de almacenamiento viene motivada desde su predecesor Megaupload debido al uso por parte de los usuarios para la compartición de material con copyright infringiendo las leyes pertinentes. Mediante los diferentes cifrados de los datos que se realizan en el sistema, el mismo pretende no tener conocimiento sobre lo que almacenan los usuarios dejándole toda responsabilidad legal a éstos. Por otro lado, no existen grandes opiniones sobre el futuro de esta plataforma debido a las condiciones de desmantelamiento de su predecesor Megaupload.

35 *Qué es y cómo funciona MEGA* 22/05/2015 <http://cosaspracticas.lasprovincias.es/como-descargar-peliculas-mega/>
36 *Funcionamiento MEGA* 22/05/2015 <http://wwwhatsnew.com/2013/01/17/como-funciona-mega-el-sucesor-de-megaupload/>

6.4. Diferencias entre los sistemas de almacenamiento

Tras el análisis realizado anteriormente de cada alternativa, a continuación se incluye una tabla resumen con las principales diferencias entre cada uno de los sistemas seleccionados para someterlos al índice de seguridad propuesto para el TFG.

Características\ Servicio	Google Drive	Dropbox	MEGA
Almacenamiento gratuito	15 GB	2 GB	50 GB
Almacenamiento gratuito extra	NO	SI	NO
Almacenamiento gratuito máximo	15 GB	24 GB	50 GB
Límite archivo	5 TB	10 GB	SIN LÍMITE
Planes pagados	SI	SI	SI
Aplicación escritorio	WINDOWS, MAC	WINDOWS, MAC, LINUX	NO
Aplicaciones dispositivos móviles	Android, iOS	Android, iOS, BlackBerry, Windows Phone, Kindle Fire	Android, iOS

Tabla 11: Diferencias sistemas de almacenamiento

Como se puede observar en la Tabla 11, los sistemas Google Drive y Dropbox muestran un mayor número de similitudes entre ellas puesto que ofrecen un tipo parecido de servicio y características de uso. Por otro lado, el servicio MEGA es el que más difiere de los tres analizados debido a su forma de uso.

6.5. Aplicación índice de seguridad

Una vez establecido el índice de seguridad y seleccionadas las alternativas que se desean analizar, se procede a la aplicación de dicho índice para la obtención de los valores finales de decisión.

Para obtener el resultado de cada alternativa, esto es el valor que propone el índice de seguridad para dicha alternativa, se van a tener en cuenta los pesos obtenidos para cada indicador a partir del método de decisión multicriterio AHP aplicado anteriormente.

Para calcular el valor ofrecido por el índice de seguridad de cada indicador en cada alternativa utilizamos la siguiente fórmula:

$$Indicador = Peso\,indicador * (\frac{Valor\,indicador}{6})$$

Donde:

- **Indicador:** resultado obtenido para cada indicador del índice en la alternativa evaluada
- **Peso indicador:** contribución que realiza dicho indicador al índice de seguridad calculado mediante la aplicación del método AHP
- **Valor indicador:** para cada indicador, resultado obtenido tras aplicar su fórmula de cálculo propuesto en el índice de seguridad

La división que se realiza entre 6 corresponde con el factor de normalización debido a la escala utilizada que se explica más adelante.

Las fórmulas propuestas de cada indicador para el cálculo del campo “Valor indicador” pueden comprobarse en las Tablas 4, 5 y 6.

A la hora de realizar los cálculos de dichas fórmulas, se ha encontrado una gran dificultad en la obtención de los datos necesarios para la aplicación de las mismas. Se trata de tres empresas de gran importancia en cuanto al almacenamiento y compartición de datos en la nube, por lo que no es de esperar que los datos en cuanto al tráfico de usuarios, número de operaciones, conexiones fallidas, número de contraseñas cifradas, etc., necesarios para el cálculo de las fórmulas propuestas sean de carácter público.

Ante este problema, se va a realizar una aplicación restringida del índice de seguridad propuesto. Para ello, a la hora de realizar el cálculo de cada indicador se va a tomar como “Valor indicador” un número aleatorio dentro la escala [1,6].

Se ha elegido esta escala en lugar de otra para centralizar la neutralidad de una escala impar. En la Tabla 12 se puede observar el significado de cada número de la escala seleccionada.

Valor escala	Significado
1	Se estima que el indicador no está en la alternativa
2	Se estima un valor muy bajo del indicador en la alternativa
3	Se estima un valor bajo del indicador en la alternativa
4	Se estima un valor medio del indicador en la alternativa
5	Se estima un valor alto del indicador en la alternativa
6	Se estima un valor muy alto del indicador en la alternativa

Tabla 12: Significados valores escala [1,6]

Una vez se tienen todos los datos necesarios para calcular cada indicador se procede a dichos cálculos. Estas operaciones quedan reflejadas en una hoja Excel que aúna todos los resultados y contiene los valores de cada indicador para cada alternativa analizada (Tabla 13).

		Alternativa de referencia		Alternativa 1: Google Drive		Alternativa 2: Dropbox		Alternativa 3: Mega	
Indicador	Peso Indicador	Valor Métrica [1,6]	Indicador=Peso Indicador * (Valor Indicador/ 6)	Valor Métrica [1,6]	Indicador=Peso Indicador * (Valor Indicador/ 6)	Valor Métrica [1,6]	Indicador=Peso Indicador * (Valor Indicador/ 6)	Valor Métrica [1,6]	Indicador=Peso Indicador * (Valor Indicador/ 6)
Integridad de datos	**0,270**		**0,270**		**0,146**		**0,153**		**0,142**
Seguridad de datos y administración del ciclo de vida de la información	**0,162**		**0,162**		**0,086**		**0,081**		**0,074**
Integridad de datos	0,022	6	0,022	6	0,022	3	0,011	2	0,007
Clasificación	0,008	6	0,008	5	0,007	4	0,005	4	0,005
Política de seguridad	0,036	6	0,036	2	0,012	4	0,024	3	0,018
Fuga de información	0,054	6	0,054	3	0,027	3	0,027	2	0,018
Propiedad/Administración	0,017	6	0,017	5	0,014	2	0,006	3	0,009
E-Commerce	0,025	6	0,025	1	0,004	2	0,008	4	0,017
Cifrado y gestión de claves	**0,042**		**0,042**		**0,024**		**0,030**		**0,027**
Generación de claves	0,005	6	0,005	4	0,003	2	0,002	5	0,004
Protección de datos sensibles	0,026	6	0,026	3	0,013	4	0,017	4	0,017
Almacenamiento y acceso	0,011	6	0,011	4	0,007	6	0,011	3	0,006
Seguridad virtual y móvil	**0,066**		**0,066**		**0,036**		**0,042**		**0,041**
Seguridad/Protección de datos	0,030	6	0,030	2	0,010	2	0,010	3	0,015
Cifrado	0,012	6	0,012	3	0,006	4	0,008	5	0,010
Almacenamiento de datos seguros en la nube	0,024	6	0,024	5	0,020	6	0,024	4	0,016
Entorno físico	**0,233**		**0,233**		**0,136**		**0,086**		**0,089**
Gestión de la continuidad	**0,083**		**0,083**		**0,063**		**0,033**		**0,030**
Servicios de centro de datos	0,034	6	0,034	3	0,017	1	0,006	3	0,017
Riesgos medioambientales	0,021	6	0,021	5	0,018	5	0,018	1	0,004
Localización equipamiento	0,028	6	0,028	6	0,028	2	0,009	2	0,009
Gestión del centro de datos	**0,043**		**0,043**		**0,028**		**0,020**		**0,010**
Políticas	0,016	6	0,016	6	0,016	3	0,008	2	0,005
Autorización de área de seguridad	0,019	6	0,019	3	0,010	2	0,006	1	0,003
Entrada no segura	0,008	6	0,008	2	0,003	4	0,005	1	0,001
Gestión de acceso	**0,107**		**0,107**		**0,045**		**0,034**		**0,049**
Puntos de control de acceso	0,041	6	0,041	1	0,007	3	0,021	2	0,014
Acceso de usuarios	0,015	6	0,015	5	0,013	2	0,005	4	0,010
Entrada no autorizada	0,051	6	0,051	3	0,026	1	0,009	3	0,026
Acceso y privilegio	**0,494**		**0,494**		**0,329**		**0,258**		**0,255**
Seguridad y recursos humanos	**0,287**		**0,287**		**0,209**		**0,149**		**0,119**
Requisitos de acceso	0,072	6	0,072	4	0,048	3	0,036	3	0,036
Identificación equipamiento	0,031	6	0,031	3	0,016	4	0,021	3	0,016
Administración de dispositivos móviles	0,042	6	0,042	5	0,035	3	0,021	4	0,028
Roles/Responsabilidades	0,095	6	0,095	5	0,079	2	0,032	2	0,032
Espacio de trabajo	0,047	6	0,047	4	0,031	5	0,039	1	0,008
Administración de identidad y acceso	**0,092**		**0,092**		**0,054**		**0,059**		**0,051**
Herramientas de auditoría de acceso	0,009	6	0,009	6	0,009	3	0,005	1	0,002
Ciclo de vida de credenciales/Administración de privilegios	0,012	6	0,012	1	0,002	5	0,010	2	0,004
Políticas y procedimientos	0,019	6	0,019	4	0,013	2	0,006	4	0,013
Segregación de funciones	0,009	6	0,009	3	0,005	4	0,006	3	0,005
Restricciones de acceso a código fuente	0,008	6	0,008	6	0,008	6	0,008	1	0,001
Acceso de terceros	0,006	6	0,006	4	0,004	4	0,004	2	0,002
Fuentes confiables	0,012	6	0,012	4	0,008	3	0,006	4	0,008
Autorización de acceso de usuarios	0,017	6	0,017	2	0,006	5	0,014	6	0,017
Infraestructura y seguridad virtual	**0,115**		**0,115**		**0,066**		**0,050**		**0,085**
Auditoría de acceso/Detección de intrusos	0,029	6	0,029	3	0,015	2	0,010	4	0,019
Seguridad en la red	0,020	6	0,020	5	0,017	2	0,007	5	0,017
Segmentación	0,011	6	0,011	4	0,007	3	0,006	3	0,006
Seguridad VMM	0,016	6	0,016	3	0,008	2	0,005	3	0,008
Seguridad inalámbrica	0,020	6	0,020	3	0,010	4	0,013	5	0,017
Contraseñas	0,019	6	0,019	3	0,010	3	0,010	6	0,019

Tabla 13: Evaluación de alternativas

En la Tabla 13 se pueden observar los valores obtenidos para cada indicador en cada alternativa tras aplicar la fórmula explicada anteriormente. Además se puede comprobar la inclusión de una alternativa de referencia en la que se obtendrían los valores máximos en cada indicador para tomarla como base de comparación. Esta tabla es el fin último del índice de seguridad propuesto para el presente Trabajo de Fin de grado ya que a través de ella se pueden evaluar las alternativas deseadas para los ámbitos de seguridad seleccionados para el índice.

6.6. Elección de alternativa

Una vez obtenidos los resultados para cada indicador, el valor final de cada alternativa se calcula mediante la siguiente fórmula:

$$\sum_{1}^{i} Indicador\,(i)$$

Donde i hace referencia a cada valor obtenido para cada indicador tras la aplicación de su fórmula.

Aplicando la fórmula anterior, y sin tener en cuenta la alternativa de referencia, se obtienen los resultados finales de cada alternativa.

Alternativa 1: Google Drive	Alternativa 2: Dropbox	Alternativa 3: Mega
0,610	0,497	0,486

Tabla 14: Valores finales alternativas

Una vez se han obtenido los resultados finales, se analiza gráficamente cómo cada alternativa difiere de la alternativa de referencia. Para ello se tienen en cuenta los ámbitos definidos en el primer nivel del AHP.

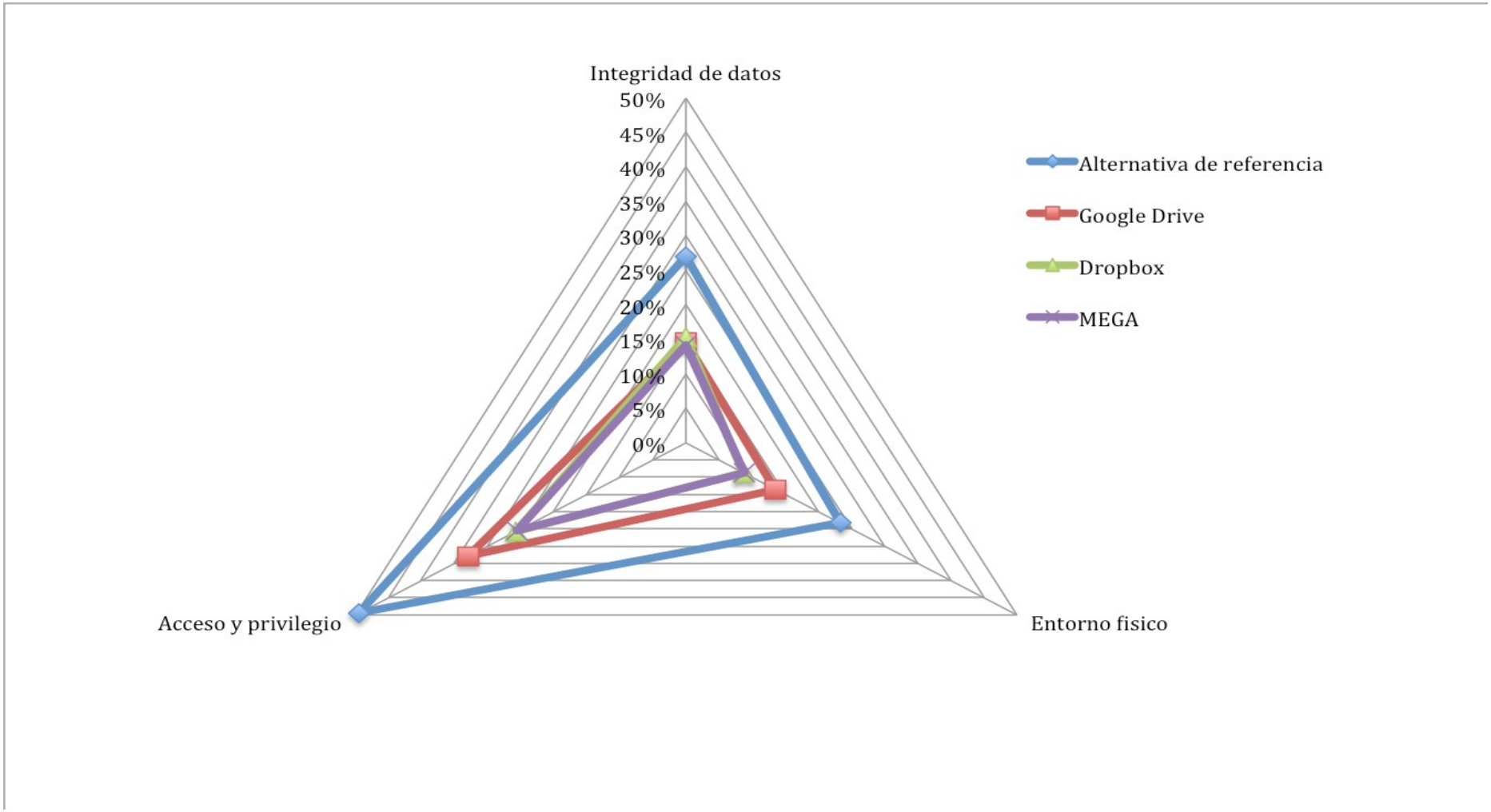


Figura 23: Resultados finales (Nivel 1)

Como se puede observar en la Figura 23, Google Drive es la alternativa más recomendable puesto que sus vértices son los que más se aproximan a la alternativa de referencia.

También se puede comprobar como el vértice de acceso y privilegio en la alternativa más valorada es el que más destaca. Por otro lado, en cuanto a las alternativas de Dropbox y MEGA, tienen un valor muy similar, siendo este el motivo por el que en el gráfico aparecen casi superpuesta una encima de la otra destacando una pequeña parte más el vértice de integridad de datos en Dropbox

Del mismo modo, se analizan gráficamente los resultados teniendo en cuenta los sub-ámbitos definidos en el segundo nivel del método AHP.

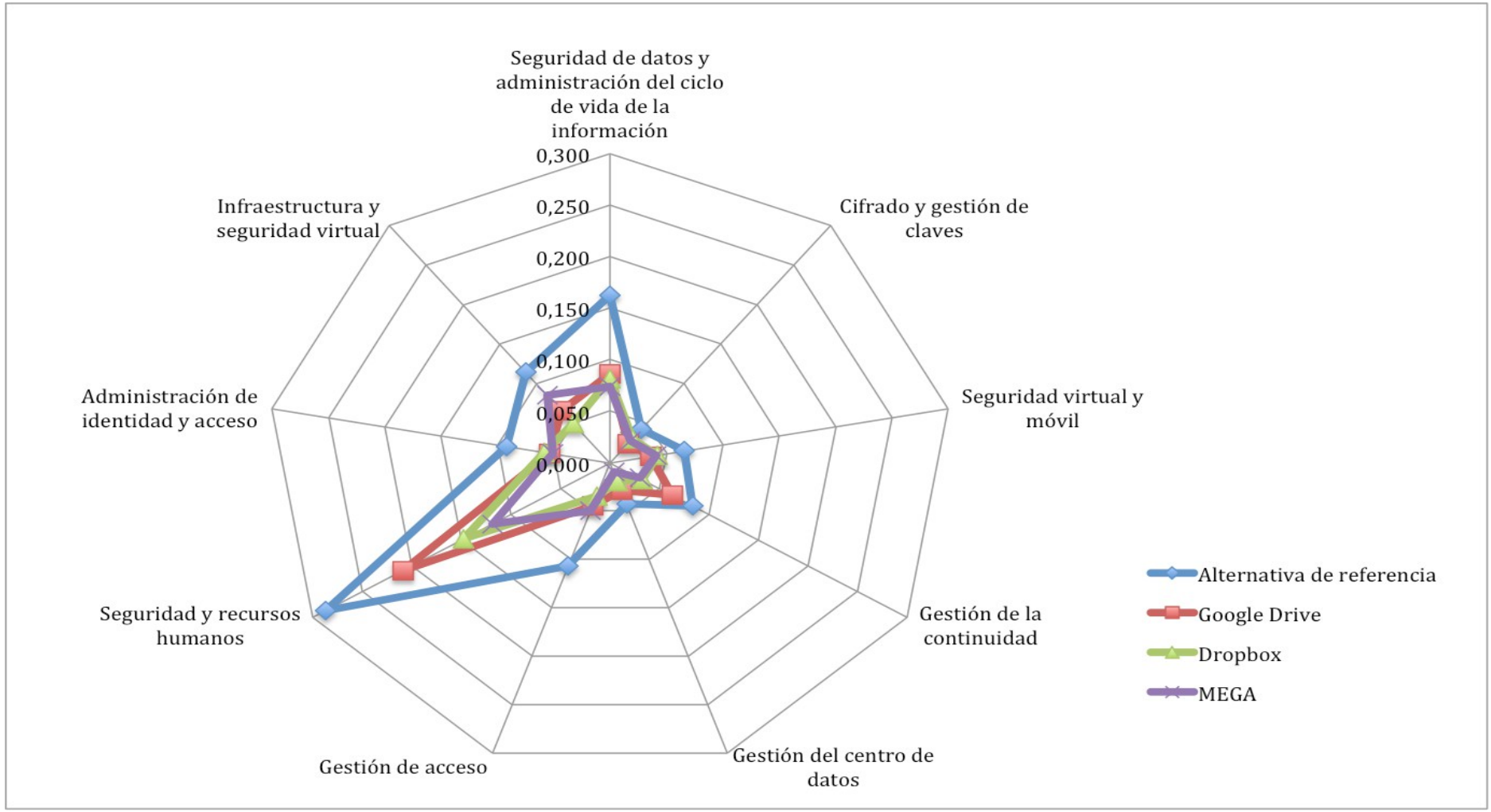


Figura 24: Resultados finales (Nivel 2)

En la Figura 24 se puede comprobar como Google Drive es la alternativa mejor valorada puesto que sus vértices son los más próximos a los de la alternativa de referencia.

En dicha figura se puede comprobar también como el vértice más importante es el que hace referencia a la seguridad y recursos humanos. Cabe destacar la gran diferencia existente entre este vértice y el de cifrado y gestión de claves que se sitúa casi en el centro del diagrama.

En este diagrama se puede observar con mayor nivel de detalle las diferencias entre Dropbox y MEGA. En la Figura 23 se puede comprobar como ambas alternativas eran prácticamente iguales, sin embargo, gracias a la Figura 24 se puede observar que la alternativa de Dropbox tiene un mayor valor ya que el vértice más valorado (seguridad y recursos humanos) se acerca más al mismo vértice de la alternativa de referencia.

Teniendo en cuenta lo expuesto anteriormente, las Tablas 13 y 14 y las Figuras 23 y 24, se puede concluir que la alternativa que mejor se ajusta a los criterios expuestos en el índice de seguridad propuesto para el presente Trabajo de Fin de Grado es **Google Drive** puesto que ofrece un valor final superior al del resto de alternativas y es la más próxima a la alternativa de referencia.

7. Conclusiones y trabajo futuro

7.1. Conclusiones del trabajo

Una vez finalizado el presente Trabajo de Fin de Grado se ha conseguido el objetivo perseguido desde su comienzo: proponer un índice de seguridad dirigido a tres ámbitos de la seguridad de la información. Desde el inicio del mismo se pretendía ofrecer dicho índice para facilitar la medición y comprobación del cumplimiento de ciertos requisitos (cada uno de los indicadores del índice) para aquellas organizaciones que deseen utilizarlo para conocer el nivel de seguridad de sus sistemas y poder realizar comparaciones entre varias alternativas.

Con el presente Trabajo de Fin de Grado se provee una herramienta que puede servir de soporte o de implmentación para estándares existentes. Además atendiendo a un objetivo técnico, mediante la realización de este trabajo se ha cubierto la necesidad expuesta de medir la seguridad de los datos en los ámbitos seleccionados. Por otro lado, mediante el caso de estudio propuesto se ha podido evaluar e interpretar los servicios elegidos que prestan servicio en la nube. Esto hace que el índice propuesto resulte útil a más niveles de la seguridad (no sólo de datos) ya que podría utilizarse para evaluar diferentes alternativas.

A través de la lectura del presente documento, el lector puede comprender la dificultad a la hora de proteger y garantizar la integridad de los datos así como algunas de las principales normas existentes hoy en día para tal fin.

Este trabajo me ha aportado la capacidad de plantear, estructurar y seleccionar la información que concierne a un proyecto de esta envergadura. Ha sido un gran trabajo de recopilación de información ya existente y planteamiento de un nuevo modelo tomando como bases otros analizados. Además, debido a la metodología utilizada se demuestra un proceso ingenieril ya que se han seguido una serie de pasos de forma iterativa: planteamiento del problema, búsqueda de información, análisis de las opciones, definición de un nuevo método, aplicación del método, selección de alternativa y análisis de resultados finales.

La realización de este trabajo, no solo me ha servido para adquirir nuevos conocimientos en el ámbito de la seguridad y la Ingeniería Informática, si no también para comprender otros aprendidos durante mis estudios y que en su momento parecían no guardar relación con lo estudiado.

A nivel personal, este trabajo ha sido un reto desde el minuto cero puesto que supone el cierre de una etapa y era el momento de aplicar conocimientos adquiridos durante la carrera.

Atendiendo al carácter del trabajo, en gran parte teórico, y pese a la apariencia tediosa que pueda arrojar, en mi caso no ha sido así sino todo lo contrario dadas mis preferencias en el ámbito de la ingeniería dirigidas hacia la investigación.

Por último, remarcar el gran esfuerzo empleado así como el gran entusiasmo durante la realización del presente Trabajo de Fin de Grado.

7.2. Trabajo futuro

Como principal línea de investigación y trabajo futuro se propone el desarrollo de este Trabajo de Fin de Grado en un ámbito más práctico puesto que éste es en su mayor parte teórico. Dado el carácter del trabajo, es inevitable tener que llevar a cabo una labor de búsqueda y recolección de información pero podría resultar práctico la implementación de un software que aúne el método de decisión multicriterio AHP de una forma más sencilla y útil para el modelo propuesto evitando así el uso de las hojas Excel.

En este caso se han analizado tres ámbitos de la seguridad de los datos e información, pero el modelo propuesto podría ser extensible a otros ámbitos de los existentes en la seguridad de la información. Podrían crearse nuevos modelos a semejanza del propuesto pero que cubran otras necesidades y ámbitos de seguridad.

Otro posible punto de desarrollo futuro consistiría en la inclusión de un mayor número de indicadores para cada ámbito de seguridad propuesto. Además podrían tenerse en cuenta un mayor número de votaciones a la hora de establecer los pesos mediante el método AHP, de modo que se incluyan nuevas percepciones de usuarios.

Dado el caso de estudio presentado en el presente Trabajo de Fin de Grado, podría proponerse como línea de investigación futura la búsqueda del valor exacto de los datos necesarios para poder aplicar las fórmulas ofrecidas para cada indicador del índice de seguridad. De este modo los resultados que se obtendrían a la hora de seleccionar una alternativa serían más precisos.

Como última línea de trabajo futuro se propone el mantenimiento actualizado del presente TFG atendiendo a las normas y actualizaciones de las mismas que se publiquen y en general a la continua revisión de toda la información que se trata durante el mismo.

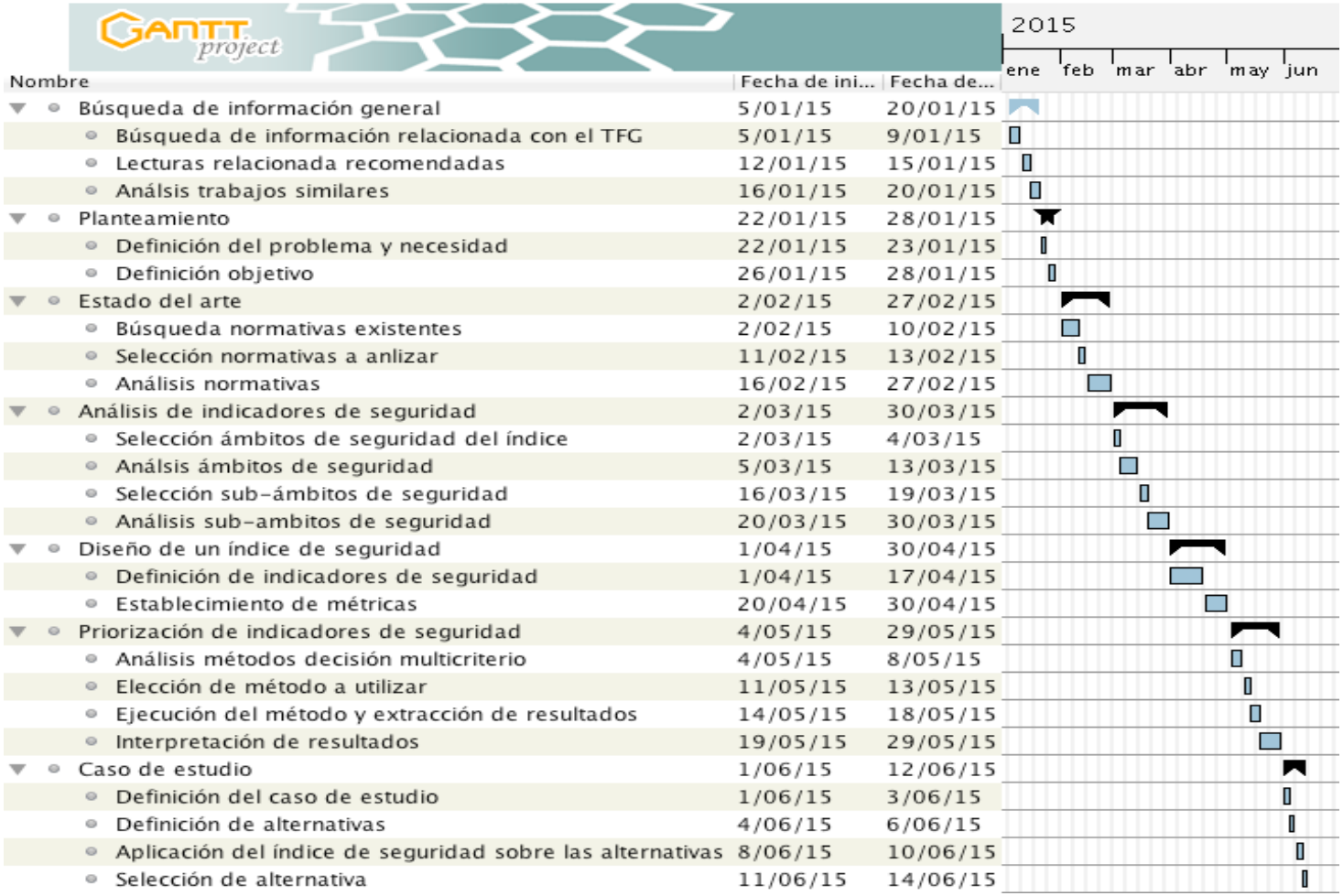
8. Planificación y presupuesto

8.1. Planificación del trabajo

En este apartado se explican las principales tareas, fases y planificación realizada para la obtención del presente Trabajo de Fin de Grado, así como el tiempo empleado en cada una de ellas. A continuación se describen las principales fases en las que se ha descompuesto el presente Trabajo de Fin de Grado y a su vez las tareas involucradas en cada un de estas etapas:

- Búsqueda de información general
  - Búsqueda de información relacionada con el TFG
  - Lecturas relacionadas recomendadas
  - Análisis trabajos similares
- Planteamiento
  - Definición del problema y necesidad
  - Definición objetivo
- Estado del arte
  - Búsqueda normativas existentes
  - Selección normativas a analizar
  - Análisis de normativas
- Análisis de indicadores de seguridad
  - Selección ámbitos de seguridad del índice
  - Análisis ámbitos de seguridad
  - Selección sub-ámbitos de seguridad del índice
  - Análisis sub-ámbitos de seguridad
- Diseño de un índice de seguridad
  - Definición de indicadores de seguridad
  - Establecimiento de métricas
- Priorización de indicadores de seguridad
  - Análisis métodos de decisión multicriterio
  - Elección de método a utilizar
  - Ejecución del método y extracción de resultados
  - Interpretación de resultados
- Caso de estudio
  - Definición del caso de estudio
  - Definición de alternativas
  - Aplicación del índice de seguridad sobre las alternativas
  - Selección de alternativa

Como se puede observar en las tareas anteriores, la mayoría se corresponden con los puntos principales del índice del presente documento. A continuación se incluye un diagrama en el que se muestra como ha sido la evolución del trabajo asi como el reparto de las tareas descritas anteriormente.



Nombre	Fecha de ini...	Fecha de...
Búsqueda de información general	5/01/15	20/01/15
Búsqueda de información relacionada con el TFG	5/01/15	9/01/15
Lecturas relacionada recomendadas	12/01/15	15/01/15
Análsis trabajos similares	16/01/15	20/01/15
Planteamiento	22/01/15	28/01/15
Definición del problema y necesidad	22/01/15	23/01/15
Definición objetivo	26/01/15	28/01/15
Estado del arte	2/02/15	27/02/15
Búsqueda normativas existentes	2/02/15	10/02/15
Selección normativas a anlizar	11/02/15	13/02/15
Análisis normativas	16/02/15	27/02/15
Análisis de indicadores de seguridad	2/03/15	30/03/15
Selección ámbitos de seguridad del índice	2/03/15	4/03/15
Análsis ámbitos de seguridad	5/03/15	13/03/15
Selección sub-ámbitos de seguridad	16/03/15	19/03/15
Análisis sub-ambitos de seguridad	20/03/15	30/03/15
Diseño de un índice de seguridad	1/04/15	30/04/15
Definición de indicadores de seguridad	1/04/15	17/04/15
Establecimiento de métricas	20/04/15	30/04/15
Priorización de indicadores de seguridad	4/05/15	29/05/15
Análisis métodos decisión multicriterio	4/05/15	8/05/15
Elección de método a utilizar	11/05/15	13/05/15
Ejecución del método y extracción de resultados	14/05/15	18/05/15
Interpretación de resultados	19/05/15	29/05/15
Caso de estudio	1/06/15	12/06/15
Definición del caso de estudio	1/06/15	3/06/15
Definición de alternativas	4/06/15	6/06/15
Aplicación del índice de seguridad sobre las alternativas	8/06/15	10/06/15
Selección de alternativa	11/06/15	14/06/15

Figura 25: Diagrama de Gantt

En la Figura 25 se puede observar un diagrama de Gantt realizado con la herramienta GanttProjetc[37] en su versión escritorio. En dicho diagrama se pueden observar las fechas de inicio y fin de cada tarea así como de forma gráfica una línea de tiempo por cada tarea que marca la duración de cada una. Además por cada fase se pueden observar las distintas tareas que la forman. Atendiendo a dicho diagrama se puede comprobar que la fecha de inicio del presente Trabajo de Fin de Grado fue el 05/01/2015 y su fecha de fin el 14/06/2015.

Cabe destacar que en cada fase, se ha redactado el apartado correspondiente del presente documento. Asimismo, no se ha incluido dentro de la planificación la preparación de la defensa y presentación del TFG puesto que se realizará en el periodo existente tras la entrega del presente documento y hasta la defensa del mismo.

8.2. Análisis económico

Para determinar el coste total de desarrollo de este Trabajo de Fin de Grado se han tenido en cuenta los diferentes tipos de costes en los que se ha incurrido durante la realización el mismo, así como el tiempo de dedicación expuesto en el apartado de planificación anterior. Los puntos a tener en cuenta para llevar a cabo el análisis económico son los siguientes:

- Tiempo de dedicación
- Costes de personal
- Costes de material: software y hardware
- Costes indirectos
- Viajes y dietas

Para menor complejidad en los cálculos se supone que es una empresa propia la que ha llevado a cabo todo el trabajo. La unidad monetaria que se utiliza es el Euro (€), teniendo en cuenta un redondeo, cuando proceda, con dos decimales.

En último lugar, para calcular el coste total del proyecto se tienen en cuenta todos los costes, impuestos aplicables y el porcentaje de ganancia deseado ligado a los riegos asumidos.

37 *GanttProject* 10/06/2015 <http://www.ganttproject.biz/>

8.2.1. Tiempo dedicado

Para llevar a cabo todos los cálculos referentes al presupuesto, se han contabilizado el número total de horas trabajadas en cada semana durante el periodo de trabajo expresado en la Figura 25. El número de horas totales dedicadas es el siguiente:

Mes	Semanas trabajadas	Horas/ Semana	Total horas
Enero	4	20	80
Febrero	4	20	80
Marzo	4	20	80
Abril	4	20	80
Mayo	4	20	80
Junio	2	20	40
TOTAL			440

Tabla 15: Tiempo dedicado

En la Tabla 15 se puede observar que el número total de horas trabajadas desde el inicio del presente TFG hasta su finalización ha sido de 440.

8.2.2. Coste de personal[38]

Para llevar a cabo el cálculo asociado al coste del personal hay que tener en cuenta a Víctor García de León González como autor del presente trabajo.

Adicionalmente han de tenerse en cuenta 50 horas de trabajo en concepto de ayuda del cotutor del Trabajo de Fin de Grado (José María Álvarez Rodríguez). Sin embargo se supone que estas horas no han generado costes adicionales al coste de personal y por este motivo no se incluyen en la Tabla 16.

En la siguiente tabla se pueden observar de forma detallada los costes asociados al personal:

Personal	Categoría	Coste hombre (€/ h)	Dedicación (horas)	Coste (€)
Víctor García de León González	Ingeniero Junior	20,00	440	8.800,00

Tabla 16: Costes de personal

En la Tabla 16 se puede observar que el coste asociado al personal por el trabajo realizado es de 8.800,00€.

38 *Bases y tipos de cotización 2015* 08/06/2015 <http://www.seg-social.es/Internet_1/Trabajadores/CotizacionRecaudaci10777/Basesytiposdecotiza36537/index.htm>

Además, es necesario tener en cuenta las bases y tipos de cotización de 2015 aplicables, en función de la categoría del personal encargado del trabajo.

En la Tabla 17 se puede observar los grupos de cotización en 2015 según la categoría a la que pertenezcan cada uno de los miembros involucrados en el proyecto.

Grupo de cotización	Categoría profesional	Base mínima (€/ mes)	Base máxima (€/ mes)
1	Ingenieros y Licenciados. Personal de alta dirección no incluidos en el artículo 1.3.c) del Estatuto de los Trabajadores	1.056,90	3.606,00
2	Ingenieros Técnicos, Peritos y Ayudantes Titulados	876,98	3.606,00

Tabla 17: Grupos de cotización

Es necesario tener en cuenta para la realización de este trabajo los tipos de cotización diferenciando entre parte asumida por la empresa y la parte asumida por el trabajador. Los tipos de cotización en 2015 pueden encontrarse en la Tabla 18.

Contingencias	Empresa (%)	Trabajadores(%)	Total(%)
Comunes	23,60	4,70	28,30
Horas extraordinarias de fuerza mayor	12,00	2,00	14,00
Resto horas extraordinarias	23,60	4,70	28,30

Tabla 18: Tipos de cotización

Con la información anterior se procede al cálculo de la cuota asociada así como el coste total del personal. Para llevar a cabo los cálculos de la Tabla 19, se ha tomado como "Base cotizada" la media aritmética entre la base mínima y máxima de cotización del grupo 2 expresadas en la Tabla 17, utilizando su tipo de cotización correspondiente (23,60%). La cuota asociada puede comprobarse en la Tabla 19.

Personal	Base máxima (€)	Base cotizada (€)	Tipo (%)	Cuota/ mes (€)	Dedicación (meses)	Coste cuota total (€)
Víctor García de León González	3.606,00	2.241,49	23,60	529,00	5,50	2.909,50

Tabla 19: Coste cuota total

Como se puede observar en la Tabla 19, el coste total de la cuota asociada al personal es de 2.909,50€.

Una vez calculado el coste de la cuota asociada se calcula el coste total del personal:

Concepto	Coste bruto (€)	Cuota total (€)	Coste total (€)
Personal	8.800,00	2.909,50	11.709,50

Tabla 20: Coste total personal

En la Tabla 20 se puede observar que el coste total de personal asciende a 11.709,50€.

8.2.3. Coste de material

La realización del presente trabajo ha conllevado una serie de gastos asociados al material utilizado. Para realizar este cálculo es necesario tener en cuenta las amortizaciones de cada una de las herramientas utilizadas. Para calcular el coste imputable asociado a cada material tendremos en cuenta lo siguiente:

- Coste equipo: Coste de la herramienta (sin IVA)
- Porcentaje de uso: Porcentaje de uso de la herramienta en el trabajo
- Dedicación: Número de meses transcurridos desde que comenzó el trabajo
- Periodo de amortización: Periodo de vida útil estimado del componente

Atendiendo a los datos anteriores, el coste imputable (en Euros) de cada herramienta se calculará mediante la fórmula expresada a continuación:

$$Coste\,imputable = \frac{Dedicación}{Periodo\,de\,amortización} \times Coste\,equipo \times Porcentaje\,de\,uso$$

Teniendo en cuenta la fórmula anterior se obtienen los siguientes resultados para costes relacionados al material (Hardware y Software) involucrado en la realización del proyecto:

Descripción	Tipo	Coste equipo (€)	Uso dedicado (%)	Dedicación (meses)	Periodo de amortización (meses)	Coste imputalbe (€)
MacBook Pro 13'' i5 2.5 GHz con 16GB	HW	1.319,00	100,00	5,50	60,00	120,91
Multifunción HP Officejet 5610	HW	120,00	100,00	5,50	48,00	13,75
Office 365 Personal	SW	69,00	100,00	5,50	12,00	31,63

Tabla 21: Coste material

Sumando todos los costes imputables de la Tabla 21, se obtiene que el coste total asociado al material utilizado en la realización del trabajo asciende a 166,28€.

8.2.4. Costes indirectos

Para la realización del presente Trabajo de Fin de Grado se ha incurrido en una serie de gastos indirectos. A continuación se desglosan dichos gastos:

Concepto	Coste/ mes (€)	Dedicación (meses)	Coste (€)
Conexión a internet por fibra óptica	70,00	5,50	385,00
Electricidad	60,00	5,50	330,00

Tabla 22: Costes indirectos

Sumando todos los costes obtenidos en la Tabla 22 se obtiene que los costes indirectos para este trabajo ascienden a 715,00€.

8.2.5. Costes totales

Una vez calculados todos los costes que conlleva la realización del presente trabajo de Fin de Grado, se procede a calcular el coste total del mismo expresado en la Tabla 23.

Concepto	Coste (€)
Coste de personal	11.709,50
Coste de material	166,28
Costes indirectos	715,00
TOTAL	**12.590,78**

Tabla 23: Coste total

El total de los costes analizados para este trabajo asciende a 12,590.78€.

Por otro lado, dejando a un lado la motivación de investigación de este trabajo, con la realización de este trabajo se pretende conseguir un beneficio. Por lo tanto al coste total obtenido anteriormente, debemos agregarle el beneficio deseado junto con el riesgo asociado:

Concepto	Porcentaje (%)	Coste total (€)	Total (€)
Beneficio	15,00	12.590,78	1.888,62
Riesgo	12,00	12.590,78	1.510,89

Tabla 24: Beneficio y riesgo

En la Tabla 24 se puede observar que el coste asociado al beneficio deseado es de 1.888,62€ y el coste asociado al riesgo es de 1.510,89€.

8.2.6. Importe total

Una vez obtenidos los datos finales, se procede al cálculo del importe final del trabajo sin IVA:

Concepto	Coste sin IVA (€)
Trabajo	12.590,78
Beneficio	1.888,62
Riesgo	1.510,89
Importe total	**15.990,29**

Tabla 25: Coste final sin IVA

En la Tabla 25 se puede observar que el coste final del trabajo sin IVA es de 15.990,29€.

Teniendo en cuenta el IVA actual reglamentario, debemos añadir el 21% al coste obtenido en la Tabla 25.

Concepto	Coste sin IVA (€)	IVA (%)	Coste con IVA (€)
Trabajo	15.990,29	21,00	19.348,25

Tabla 26: Coste final con IVA

Por lo tanto, como se puede observar en la Tabla 26, el coste final de la realización de este trabajo de Fin de Grado, teniendo en cuenta todos los costes implicados y los impuestos vigentes asciende a 19.348,25€ (Diecinueve mil trecientos cuarenta y ocho Euros con veinticinco céntimos).

9. Bibliografía

A continuación se listan todos los recursos electrónicos utilizados para la realización del presente Trabajo de Fin de Grado:

[1] "AXELOS", 26/02/2015, <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>

[2] Héctor Acevedo Juarez, "Administración de servicios de TI", 26/02/2015, <http://www.magazcitum.com.mx/?p=50>

[3] "QRPInternational", 26/02/2015, <http://www.qrpinternational.es/index/itil/what-is-itil>

[4] APM Group, "Ruta de certificación ITIL", 26/02/2015, <http://www.blauconsulting.com/itil/mapa-de-certificacion-itil.html>

[5] Osiatis, "ITIL – Gestión de servicios TI", 26/02/2015, <http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/proceso_gestion_de_la_seguridad/aplicacion_medidas_de_seguridad.php>

[6] "Turevisorfiscal", 28/02/2015, <http://turevisorfiscal.com/que-es-el-cobit/>

[7] APMG, "COBIT5 Qualifications", 28/02/2015, <http://www.apmginternational.com/en/qualifications/cobit5/cobit5.aspx>

[8] Joan Puig, Sergi Blanco "Estándar para el buen gobierno de los sistemas de la información", 28/02/2015, <http://www.marblestation.com/?p=645>

[9] Portal Administración Electrónica del Estado, "Metodología de análisis y gestión de riesgos de los Sistemas de Información", 02/03/2015, <http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VU4kCtPtmko>

[10] "Funcionamiento metodología Magerit", 02/03/2015, <https://www.ccn-cert.cni.es/publico/herramientas/pilar-5.3.1/

[11] "Metodología de análisis y gestión de riesgos de los Sistemas de Información", 02/03/2015, <https://seguridadinformaticaufps.wikispaces.com/MAGERIT>

[12] ISO ORG, "ISO Standards", 01/03/2015, <http://www.iso.org/iso/home/standards.htm>

[13] "La serie ISO27000", 01/03/2015, <http://www.iso27000.es/download/doc_iso27000_all.pdf>

[14] "ISO 27001: Gestión de la Seguridad de la Información", 02/03/2015, <http://www.normas-iso.com/iso-27001>

[15] ISOTools, "Medición de la Seguridad de la Información", 03/03/2015, <http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/>

[16] CCMv3, "Cloud Controls Matrix Version 3", 10/03/2015, <https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx >

[17] "Matriz de controles Version 3", 10/03/2015, <https://cloudsecurityalliance.org/initiatives/ccm/ >

[18] "Control de acceso a la información", 18/03/2015, <http://www.ongei.gob.pe/publica/metodologias/lib5007/313.HTM>

[19] Roberto Woo Borrego, "Control de acceso", 18/03/2015, <http://www.alapsi.net/images/Capsula_1_de_4_ca.pdf>

[20] Antonio Villalón, "Seguridad física", 15/03/2015, <http://www.segu-info.com.ar/fisica/seguridadfisica.htm>

[21] Markus Erb, "Seguridad de la información y protección de datos", 12/03/2015 <https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/>

[22] Hugo Roche, Constantino Viejo, "Análisis multicriterio", 25/04/2015, <http://www.ccee.edu.uy/ensenian/catmetad/material/MdA-Scoring-AHP.pdf>

[23] Sergio A. Berumen, "Decisión multicriterio", 25/04/2015, <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-35922007000200004>

[24] Rafael Caballero Fernández, Mónica Hernández Huelín, "Ponderación Lineal", 25/04/2015, <http://www.uv.es/asepuma/XI/07.pdf>

[25] Sixto Ríos-Insua, Alfonso Mateos, Antonio Jimenez, "Teoría de la utilidad", 26/04/2015, <http://www.uv.es/asepuma/recta/extraordinarios/Vol_01/03t.pdf>

[26] Eduardo Bustos Farias, "Métodos multicriterio de ayuda a la decisión", 26/04/2015, <http://www.angelfire.com/ak6/publicaciones/congreso_it_zacatepec.pdf>

[27] "La decisión con apoyo cuantitativo", 25/04/2015, <http://tic.uis.edu.co/ava/pluginfile.php/246973/mod_resource/content/1/M%C3%A9todo%20AHP.pdf>

[28] Alberto Castro, "Servicios de almacenamiento en la nube", 15/05/2015, <http://computerhoy.com/listas/software/mejores-servicios-gratuitos-almacenamiento-nube-8518>

[29] Pablo Romero, "Almacenamiento en la nube", 15/05/2015, <http://www.elmundo.es/elmundo/2012/04/25/navegante/1335354932.html>

[30] Google, "Información Google Drive", 15/05/2015, <https://support.google.com/drive/answer/6558?hl=es>

[31] Dropbox, "Dropbox help", 20/05/2015, <https://www.dropbox.com/help>

[32] P. Rodríguez, "Dropbox empresas", 20/05/2015, <http://www.xatakaon.com/almacenamiento-en-la-nube/dropbox-lanza-su-version-para-empresas-con-interesantes-novedades>

[33] Manuel Mateos, "Cuidado con Dropbox", 20/05/2015, <http://www.genbeta.com/herramientas/cuidado-con-dropbox-podrian-tener-posibilidad-de-acceder-a-tus-archivos>

[34] Dropbox, "Dropbox pricing", 20/05/2015, <https://www.dropbox.com/business/pricing>

[35] "Qué es y cómo funciona MEGA", 22/05/2015, <http://cosaspracticas.lasprovincias.es/como-descargar-peliculas-mega/>

[36] Juan David Quiñonez, "Funcionamiento MEGA", 22/05/2015, <http://wwwhatsnew.com/2013/01/17/como-funciona-mega-el-sucesor-de-megaupload/>

[37] "GanttProject", 10/06/2015, <http://www.ganttproject.biz/>

[38] Seguridad Social, "Bases y tipos de cotización 2015", 08/06/2015, <http://www.seg-social.es/Internet_1/Trabajadores/CotizacionRecaudaci10777/Basesytiposdecotiza36537/index.htm>

Adicionalmente se han consultado los siguientes libros:

[39] Cristina Merino Bada, Ricardo Cañizares Salas, "Implantación de un sistema de gestión de seguridad de la información según ISO 27001", PC Editorial, Diciembre 2011

[40] Javier Areito Bertolín, "Seguridad de la información. Redes, informática y sistemas de información", Paraninfo, Edición 2008

[41] Ana Andrés Álvarez, Luís Antonio Gómez Fernández, "Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes", AENOR Ediciones, Abril 2009

[42] Anderson, Sweeney y Williams, "Métodos cuantitativos para los negocios", Septima Edición

[43] Thomas Saaty, "The Analytical Hierarchy Process", McGraw Hill, 1998

ANEXO A: EXTENDED ABSTRACT

A1. Introduction

This chapter contains a brief introduction to the Final Deegre Work. To do so it will be exposed the existing problem, the motivation which made me do this work and the objective followed.

A1.1. Problem and necessity

Personal data is something which everybody must deal with every day. Most of the transactions involving this kind of data are done by computer applications or usually in a networ-based environment. This is a big issue because in some ocations we give to these applications all our personal details without thinking about the consequences if that information is revealed to other people.

All the applications that deal with sensitive data should guarantee a minimum of security and confidentiality in order to ensure the user that his/her details will be used in a good way. Moreover, this kind of applications should be controlled and also under legal framework, so that their responsibles ensure a correct operation and tratment of the information as well as the responsability for a possible malpractice.

Due to threats and vulnerabilities that exist around data protection, it is neccessary to control applications which deal with this kind of information. That is why it has been thought necessary to do this research aimed to analyze the issue and establish a security index that includes measurable indicators to ensure data protection in several security areas.

A1.2. Work motivation

The motivation for this work stems from the curiosity of knowing how sensitive data is handled in different areas of IT security. As a potential user of internet, I am requested private information daily, and sometimes I give it warily, because I don't have any proof that ensures me that fraudulent use of it will not be made or that it will be revealed to third parties. I find it just as interesting to know how the level of security in IT in existing applications or organizations can be measured.

A1.3. Objective

This work proposes a security index which seeks to resolve, as far as possible, the doubts around how to measure security within a security process to ensure data integrity.

In order to reach this major objective, the existing standards ITIL, COBIT, MAGERIT and ISO will be analyzed to compare which security area covers each one.

The main outcome of this work is a security index. This index will be composed of several measurable and applicable indicators to data processing to establish the level of contribution of the selected indicators. In order to calculate each of the contributions to the security index of each indicator a multicriteria decision method will be used.

A2. Project abstract

The objective of this project is to propose a security index applicable to different areas of security. To get to that point, it is needed to perform a number of steps.

First of all, it is necessary to do a research in order to know if there are other similar alternatives. Taking this into account, the existing standards ITIL, COBIT, MAGERIT and ISO will be analyzed.

A2.1. ITIL

ITIL is a collection of knowledge and practices for managing services, development and operations with IT. This methodology proposes a set of management procedures that intend to help organizations to achieve quality and efficiency in IT operations. These processes have been developed as a guide covering all infrastructure, development and IT operations .

The ultimate goal of ITIL is to advocate for IT services aligned with business needs and support their processes. It also provides guidance to both organizations and private users, on the use of IT in business transformation and growth.

ITIL is detailed in some publications, each one focused at a particular area of IT management. The latest revision of ITIL has led to a new set of publications known as ITIL Version 3.

ITIL certification schema proposes a series of certifications aimed at different areas of ITIL best practices with different depth degrees and details. Qualification levels structure gives users some flexibility in relation with the different disciplines and areas of ITIL. Within this certification schema there are four levels, each one with different details. These levels are: Foundation, Intermediate, Expert and Master.

A2.2. COBIT

COBIT framework is internationally accepted as a good practice for control and IT maintenance and associated risks. Using COBIT it is possible to evaluate the ability of the system to generate relevant and reliable information to the attainment of the objectives set out in an organization.

COBIT establishes a model that evaluates the following aspects:

- Processes involved in the organization
- IT resources within the organization
- Information criterios

In the last version of COBIT (COBIT 5) which was edited by ISACA, there are three levels in which you can specialize, each one ensuring great knowledge of this method. These levels are: Foundation, Implementation and Assesor.

This versión pursues the creation of a practical guide to ensure safety in the organization. Within the scope of information security and data integrity, COBIT can reduce risks through proper management.

A2.3. MAGERIT

Magerit is a methodology of analysis and risk management for information systems developed by the CSAE to minimize the implementation and use risks of IT focused on public administration. This methodology incumbent on both the digitized information and computer systems that treat it.

ICT use entails large benefits for citizens but also provokes risks that must be managed with security measures that sustain the confidence of service users.

Magerit methodology pursues a methodical approach to the problem that arises when analyzing risks. Magerit objectives are:

- Give knowledge of the existence of risks and the need to minimize the effects of them to the responsibles for information systems.
- Propose a systematic method for analyzing risks.
- Planning measures and contingency plans for risks.
- Preparation for processes of organizational assessment: audition, certification or accreditation.

Magerit structure is divided in three models:

- Elements: provides system components (assets, threats, vulnerabilities, impact, risk and safeguard).
- Events: interrelated and the same with time.
- Processes: describes the security process into four stages (planning, risk analysis, risk management and safeguard selection).

A2.4. ISO

ISO is a worldwide organization that integrates various standardization methods of several countries. Its purpose is the creation and promotion of international standards covering most business environments. Its main function is the standardization of international standards for products and business security.

Information security and data integrity is controlled by the ISO/IEC 27000 standard. This standard is about:

- Preserve data confidentiality of the organization.
- Ensure data integrity of the organization.
- Ensure the availability of all information of the organization.

In the 27000 series there are some rules focused on safety management. Taking into account the motivation of this paper, there will be analyzed some rules: ISO-27000, ISO-27001, ISO-27002, ISO-27003 and ISO-27004.

Addressing the objective and structure of the ISO-27001, it is directly related to the main theme of this work that aims to establish a security index with a number of metrics (indicators) that must be verifiable to quantify the security level of an organization. For this reason, this standard has been taken as a reference for the establishment and selection of each of the indicators proposed in the index.

A2.5. Analysis of security indicators

After analyzing the data security and data integrity on the existing methods, there is a personal motivation to find some measurable and auditable indicators for someone who does not have an extensive knowledge of IT for the preparation of a security index. Finding this model will help an organization to determine the level of security that can offer to its customers in the security areas selected.

Once the existing methods are analyzed, it is going to be proposed a list of measurable indicators to cover three areas of information security. The areas chosen for the security index are:

- Access and privilge
- Physical environment
- Data integrity and privacy loss

For each of these areas, it has been done a división in sub-areas taking into account the relations between indicators in each one.

As indicated above, in order to create the security index, it has been taken based on the standard ISO-27001. From an analysis of its objectives and controls, there has been selected different security areas for the classification of the indicators that are evaluated in the index.

Moreover, for the realization of this section it has been taken based on the matrix "Cloud Controls Matrix Version 3.0 " (CCMv3) where there is a division in some security areas and each one has a series of indicators. In some cases these indicators had a proposed metric for evaluation. From this matrix and the analyzed methods (mainly ISO-27001) it has been made a division and determinadcion of the security indicators for each area.

The different areas and sub-areas selected for the realization of the desired security index are listed now.

A2.5.1. Access and privilege

In this area there are mainly those indicators related to the management of information by different users, since access to the platforms, permitions or infrastructures used. Also this area has been divided into sub-areas in order to classify in a better way each one of the indicators.

1. Data security and human resources
   - 1.1. Access requirements
   - 1.2. Equipment identification
   - 1.3. Mobile devices administration
   - 1.4. Roles/Responsabilities
   - 1.5. Workspace

2. Identity and access management
   - 2.1. Access auditing tolos
   - 2.2. Credentials lifecycle/Privileges administration
   - 2.3. Policies and procedures
   - 2.4. Functions segregation
   - 2.5. Source code restriction Access
   - 2.6. Third part Access
   - 2.7. Reliable sources
   - 2.8. Users access authorization

3. Virtual infrastructure and security
   - 3.1. Access audit/Intrusion detection
   - 3.2. Network security
   - 3.3. Segmentation
   - 3.4. VMM security
   - 3.5. Wireless security
   - 3.6. Passwords

A2.5.2. Physical environment

In the area of physical environment, there are all indicators refered to the scenario in which data is physically located. Within this area, just as with the previous, it has been made a subdivision in order to make a more accurately clasification of the indicators.

1. Business continuity management
   1.1. Data center services
   1.2. Environmental risks
   1.3. Equipment location

2. Data center mangement
   2.1. Policies
   2.2. Security area athoritation
   2.3. No-safe entry

3. Access management
   3.1. Access control points
   3.2. Users Access
   3.3. Unauthorized entry

A2.5.3. Data integrity

In this area there are those indicators that are referenced to data, from storage, encryption or virtual security. There is a subdivisión so that each indicator fits best in them.

1. Data security and information lifecycle
   1.1. Data integrity
   1.2. Clasification
   1.3. Security policy
   1.4. Information leakage
   1.5. Property/Administration
   1.6. E-commerce

2. Encryption and key management
   2.1. Key generation
   2.2. Sensitive data protection
   2.3. Storage and Access

3. Virtual and mobile security
   3.1. Security/Data protection
   3.2. Encryption
   3.3. Secure data storage in the cloud

A2.6. Designing a security index

Taking into account each of the indicators defined above, for each one there is going to be a definition and a measure. Thanks to these measures, each one can be evaluated by calculating its value. If each one is evaluated, there would be a final value for the security index proposed in this work.

A2.7. Security indicators priorization

It has been created a security index focused on three different areas of data preservation within IT. In this index there have been established and defined some measurable indicators in order to obtain a value for each.

To evaluate different alternatives with the security index, it is neccessary to know how each indicator contributes for determining the most valuated area and establish a hierarchy among them.

In order to obtain the weight (contribution) og each indicator, it is going to be used the multi-criteria decision method AHP (Analytic Hierarchy Process) because it fits perfectly with the kind of problem analyzed.

In this method, it is very important the figure of the “decisions maker”, these people are the ones who do their voting about each indicator. The decision maker must establish the importance of each objective (in this case each security indicator), so that then a hierarchical structure can be established which is used to analyze different alternatives.

The result is a classification of the alternatives indicating the value of each one according to the proposed security index and therefore provides the recommended alternative.

The main feature of this method is that the problema analyzed is modeled by a hierarchy in a tree in whose top vertex is the goal to achieve, and at the base the alternatives evaluated. At the intermediate levels (which can form a new hierarchy) it can be found the criteria in which the decisons are based on.

Another interesting point in AHP method, is that in each level in the hierarchy comparisons between pairs of elements (security indicators) are made. This comparison is based on the preference of the decision maker who will show a greater interest to an indicator than to another.

Once each contribution to the upper leve lis evaluated it is proceed to calculate the overall contribution of each alternative to the main objective.

The information obtained through this method can be redundant or inconsistent due to the number of votes taken into account. However this redundancy is which improves the accuracy of the valuations avoiding a greater number of errors.

To make the voting by the decision-makers there are going to be used some existing Excel sheets. Once these decisions are made and following the described steps, final results can be obtained. In this case, there have been two votes, one with a user-level vision and another with technical vision.

Tis idea is sustained by the table below which shows a summary with the results obtained after the application of the AHP method for the classification in the security areas chosen.

Indicator	Weight
Access and privilege	**0,494**
Data security and human resources	0,287
Identity and access management	0,092
Virtual infrastructure and security	0,115
Physical environment	**0,233**
Business continuity management	0,083
Data center mangement	0,043
Access management	0,107
Data integrity	**0,270**
Data security and information lifecycle	0,162
Encryption and key management	0,042
Virtual and mobile security	0,066

Tabla 27: AHP results

In the previous table it can be observed each area and sub-area contibution to the security index.

A2.8. Practical study

Once the security index is established, it can be used to analyzed different alternatives in order to know which one fits better according to the selected security areas of the index.

In this case, there are going to be evaluated different storage systems in the cloud. The selected systems are: Google Drive, Dropbox and MEGA.

Now it can be observed in the following table the values obtained for each alternative.

Alternative 1: Google Drive	Alternative 2: Dropbox	Alternative 3: Mega
0,610	0,497	0,486

Tabla 28: Final results

According to the previous table, it can be affirmed that Google Drive is the best option according to the security index proposed because it is the alternative with the higher value.

A3. Conclusions and future work

A3.1. Conclusion

Once completed this work it has been reached the initial objective: proposng a security index focused into three different areas of security involving IT. Since the beginning of this work, it was intended to offer that security index in order to facilitate the measurement and verification of some requirements (each security indicator included in the index) to those organizations interested in knowing the level of security offered by its products.

This work provides a security index that can help to the existing standards. With its realization it has been covered the necessity to measure data security in the exposed areas. With the case of study done, it has been measured the security existing in three important data storage services.

Through the reading of this document, the reader will understand the difficulty in protecting and ensuring the confidentiality of data as well as some of the major existing methods for this purpose.

This work has given me the ability to raise, organize and select information concerning a project of this size. It has been done a great work of collecting existing information and a new method based on others analyzed. Moreover, due to the methodology used it shows an engineering process during the work because it is used as an iterative process: problema stablement, information search, analysis of

the alternatives, definition of a new method, application of that method and alternative selection and analysis of final the results.

Doing this job, has not only given me the possibility of acquiring new knowledge about security and computer engineering, but also it has made me understand some information learnt during my studies that in that moment didn't seem very useful.

On a personal level, this work has been a big challenge since the begining because it means closing a stage and it was time to apply the knowledge acquired during the degree.

Atending to the nature of the work, mostly theoretical, and despite the dull look it can provoke, in my case it was the contrary because of my personal preferences on the different areas in computer engineering directed towards research.

Finally I would like to emphasize the great effort made to do this work trying to offer an output with the expected quality.

A2.8. Future work

As main research work and future development of this work, it is proposed the development of this work in a more practical way because this one is mostly theoretical. Atending the nature of the work, it is impossible not to do an information research labour. It could be very useful to implement a software which includes the proposed multi-criteria method AHP so that the use of Excel sheets could be avoided.

In this case, there have been analyzed three security areas involving data and information. This method could be extensible to others areas existing in security subject. Others methods could be created following the structure of the proposed one.

Taking into account the case of study presented in this work, it could be proposed as a future work the search of the exact value of each indicator instead of an estimation so that the meassures proposed could ve calculated. This way, the final result obtained would be more accurate.

Finally, as a future work, it would be recommended to mantain this work updated with the latest versions of the methods involved and the information exposed.